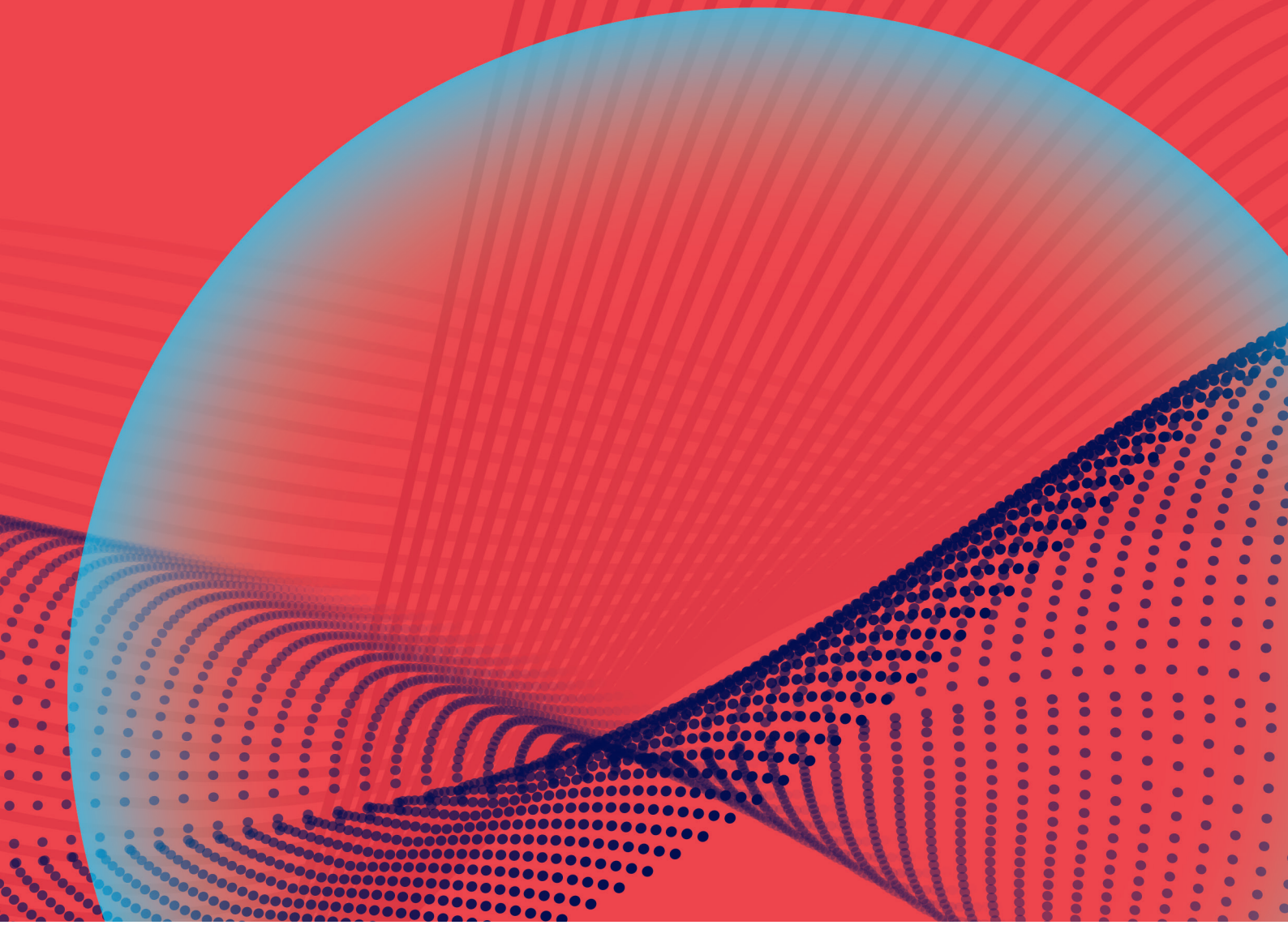
GLOBAL FORUM ON
TRANSPARENCY AND EXCHANGE OF INFORMATION FOR TAX PURPOSES

Toolkit for the Implementation of the Standard for Automatic Exchange of Financial Account Information



german cooperation
DEUTSCHE ZUSAMMENARBEIT

Implemented by
giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

OECD
BETTER POLICIES FOR BETTER LIVES

Table of contents

Abbreviations and acronyms 4

Preface 6

About this toolkit 8

1. INTRODUCTION 9

1.1. A new international standard on transparency and exchange of information for tax purposes 9

1.1.1. The history of automatic exchange of financial account information 9

1.1.2. The basics of the standard on automatic exchange of financial account information 10

1.2. Benefits of implementing the standard on automatic exchange of financial account information 11

1.2.1. Significant boost to domestic revenue and taxpayer compliance 12

1.2.2. Improved transparency on financial flows investment 12

1.2.3. Synergies with other tax transparency initiatives 13

2. OVERVIEW OF THE IMPLEMENTATION OF THE STANDARD AND ITS MONITORING AND ASSESSMENT FRAMEWORK 14

2.1. Reference documents and tools for the implementation of the Standard 14

2.1.1. The standard for Automatic Exchange of Financial Account Information in Tax Matters 15

2.1.2. The Implementation Handbook 15

2.1.3. The Common Reporting Standard related Frequently Asked Questions 15

2.1.4. The Guide on Promoting and Assessing Compliance by Financial Institutions 15

2.1.5. The Automatic Exchange Portal 15

2.2. Key building blocks for the implementation of the standard on automatic exchange of financial account information 17

2.2.1. Legislative framework 18

2.2.2. Administrative and IT capacity 18

2.2.3. Confidentiality and data safeguards 19

Table of contents

2.3. High-level architecture of the Common Reporting Standard 19

2.3.1. The scope of the Common Reporting Standard 20

2.3.2. The due diligence procedures 21

2.3.3. Information to be reported 22

2.3.4. Effective implementation 24

2.4. The monitoring and peer review processes of the implementation of the standard on automatic exchange of financial account information 24

2.4.1. The monitoring process 26

2.4.2. The peer review process 26

3. IMPLEMENTATION STRATEGY 33

3.1. Committing to implement the Standard by a specific date 33

3.1.1. Defining a realistic date for the first exchanges under the Standard 34

3.1.2. The commitment process 34

3.2. Developing and implementing the strategy 35

3.2.1. Setting up an organisational framework 35

3.2.2. Strategic decisions 36

3.3. The support provided by the Global Forum Secretariat 40

4. VOLUNTARY DISCLOSURE PROGRAMME 41

4.1. What is a voluntary disclosure programme? 41

4.2. Why consider a disclosure programme as part of the implementation strategy of the Standard? 42

4.3. Core principles of voluntary disclosure programmes 43

4.4. How to set up a successful programme? 43

4.4.1. Preliminary considerations 43

4.4.2. Designing the programme 45

4.4.3. Implementing the programme 48

4.4.4. Recommended legislation content and country experience 50

5. INTERNATIONAL LEGAL FRAMEWORK 53

5.1. The Convention on Mutual Administrative Assistance in Tax Matters 53

5.2. The Multilateral Competent Authority Agreement on Automatic Exchange of Financial Account Information 54

5.2.1. Overview of the provisions of the Competent Authority Agreement on Automatic Exchange of Financial Account Information 54

5.2.2. Signing and activating the Multilateral Competent Authority Agreement on Automatic Exchange of Financial Account Information 57

5.3. Interaction between the Convention on Mutual Administrative Assistance in Tax Matters and the Multilateral Competent Authority Agreement on Automatic Exchange of Financial Account Information 59

5.3.1. Date of effect of the Convention on Mutual Administrative Assistance in Tax Matters 60

5.3.2. Diverging tax year 61

5.3.3. Declaration on the effective date for exchanges of information under the Multilateral Competent Authority Agreement on Automatic Exchange of Financial Account Information 61

6. DOMESTIC LEGAL FRAMEWORK 63

6.1. Step 1: Structuring the legislative framework 64

6.1.1. Step 1A: How should a jurisdiction transpose the due diligence and reporting requirements: "copy out" or "reference" method? 64

6.1.2. Step 1B: How should the legal framework be structured across primary and secondary legislation, and guidance? 68

6.1.3. Step 1C: Can a jurisdiction rely on existing domestic legislation? 71

6.2. Step 2: What other measures are needed to ensure effective implementation of the Standard? 74

6.2.1. Dates of due diligence requirements 75

Table of contents

6.2.2. Filing requirements 77
6.2.3. Record-keeping requirements 79
6.2.4. Access and information gathering powers 81
6.2.5. Penalties 81
6.2.6. Anti-circumvention 84
6.2.7. Overriding pre-existing secrecy or confidentiality provisions 86
6.2.8. Strong measures to ensure self-certifications are always obtained 87

6.3. Step 3: What optional provisions can be implemented? 88

6.3.1. Jurisdiction-specific Non-Reporting Financial Institutions 89
6.3.2. Jurisdiction-specific Excluded Accounts 92
6.3.3. Alternative approach to calculating account balances 95
6.3.4. Use of reporting period other than calendar year 95
6.3.5. Phasing in the requirement to report gross proceeds 96
6.3.6. Requirement to file nil returns 96
6.3.7. Use of third party service providers by Financial Institutions 96
6.3.8. New Account due diligence procedures for Preexisting Accounts 97
6.3.9. High Value Account due diligence procedures for Lower Value Accounts 98
6.3.10. Residence address test for Lower Value Accounts 99
6.3.11. Exclusions for Preexisting Entity Accounts of USD 250 000 or less 99
6.3.12. Alternative documentation procedure for certain Group Insurance Contracts or Annuity Contracts 100
6.3.13. Allowing existing standardised industry coding systems in due diligence procedures 101
6.3.14. Currency translation 102
6.3.15. Currency election 103
6.3.16. Expanded definition of Preexisting Account 103
6.3.17. Expanded definition of Related Entity 104
6.3.18. Grandfathering of bearer shares issued by Exempt Collective Investment Vehicle 105
6.3.19. Controlling Persons of a trust 105
6.3.20. The wider approach and similar options 106

7. ENSURING EFFECTIVE IMPLEMENTATION 108

7.1. Administrative compliance framework 108

7.1.1. Compliance strategy 108
7.1.2. Encouraging voluntary compliance 109
7.1.3. Conducting compliance audits and inspections 110
7.1.4. Applying sanctions as appropriate 112
7.1.5. Collaborating with exchange partners on compliance and enforcement 112

7.2. Exchanging information effectively 112

7.2.1. Developing an IT solution: the AEOI portal 113
7.2.2. Obtaining information from Financial Institutions 120
7.2.3. Preparing data for the partners 124
7.2.4. Exchanging the CRS data with partner jurisdictions 125

8. ENSURING EFFECTIVE USE OF THE DATA 131

8.1. Data treatment 132

8.1.1. Tax identification number 133
8.1.2. Other identification information 134
8.1.3. Domestic databases 134
8.1.4. Cleansing and parsing process 135
8.1.5. Nature of CRS data 136

8.2. Data matching 138

8.2.1. Automatic matching 139
8.2.2. Fuzzy matching 139
8.2.3. Manual matching 141
8.2.4. Unmatched data 142

8.3. Data analysis 143

8.3.1. Risk analysis 143
8.3.2. Reviewing taxpayer compliance 145
8.3.3. Enhancing taxpayer compliance 148

ANNEXES 151

Annex A. Glossary of concepts 152

Annex B. Substantive additional detail 156

Annex C. Model rules based on the "reference" method 158

Annex D. Documentation 170

Annex E. Donors of the Global Forum capacity-building programme 174

Abbreviations and acronyms

AEOI	Automatic Exchange of Information
AML/CFT	Anti-Money Laundering and Counter Financing of Terrorism
API	Application Programming Interface
APRG	AEOI Peer Review Group
APRG+	AEOI Peer Review Group +
BCAA	Bilateral Competent Authority Agreement
BIAC	Business and Industry Advisory Committee to the OECD
BMZ	German Federal Ministry for Economic Cooperation and Development (*Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung*)
CAA	Competent Authority Agreement
CB	Co-ordinating Body
CbC	Country-by-Country
CIV	Collective Investment Vehicle
CR	Core Requirement
CRS	Common Reporting Standard
CRS MCAA	Multilateral Competent Authority Agreement on Automatic Exchange of Financial Account Information
CRS-AEOI	Automatic Exchange of Financial Account Information
CRS-AEOI standard	Standard for automatic exchange of financial account information or Standard
CTS	Common Transmission System
DTC	Double Taxation Convention
EOI	Exchange of Information
FAQs	Frequently Asked Questions
FATCA	Foreign Account Tax Compliance Act
FATF	Financial Action Task Force
FTA	Forum on Tax Administration
G20	The Group of Twenty
GIIN	Global Intermediary Identification Number
GIZ	Deutsche Gesellschaft für Internationale Zusammenarbeit
Global Forum	Global Forum on Transparency and Exchange of Information for Tax Purposes
HNWI	High-Net-Worth Individual
HTTPS	Hyper Text Transfer Protocol Secure
IFC	International Financial Centre

Abbreviations and acronyms

IFF	Illicit Financial Flow
IGA	Intergovernmental Agreement
ISM	Information Security Management
KYC	Know Your Customer
MAAC	Convention on Mutual Administrative Assistance in Tax Matters
MDR	Mandatory Disclosure Rules on CRS Avoidance Arrangements and Opaque Offshore Structures
Model CAA	Model Competent Authority Agreement
NDA	Non-Disclosure Agreement
NFE	Non-Financial Entity
NTJ	Exchanges on Substantial Activities in No or Only Nominal Tax Jurisdictions
OECD	Organisation for Economic Co-operation and Development
RPA	Robotic Process Automation
SFTP	Simple File Transfer Protocol
SLA	Service Level Agreement
SR	Sub-requirement
TIEA	Tax Information Exchange Agreement
TIN	Tax Identification Number
ToR	Terms of Reference
UK	United Kingdom
US	United States
VDP	Voluntary Disclosure Programme
XML	Extensible Mark-up Language

Preface

María José Garde
Chair
Global Forum on Transparency and Exchange of Information for Tax Purposes

Zayda Manatta
Head of the Secretariat
Global Forum on Transparency and Exchange of Information for Tax Purposes

Günther Taube
Head of Sector Programme Good Financial Governance
Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

A call of the G20 leaders on the international community to strengthen transparency and exchange of information by facilitating transparency on financial accounts held abroad was made in 2014. This led to the OECD, working together with G20 countries and in close co-operation with the European Union, as well as other stakeholders, to develop the international Standard for Automatic Exchange of Financial Account Information in Tax Matters (CRS-AEOI standard or Standard).[1]

The CRS-AEOI standard is a form of automatic exchange of information (AEOI) and aims to equip tax authorities with an effective tool to tackle offshore tax evasion by providing a greater level of information on their residents' wealth held abroad. Offshore tax evasion is not only a budgetary issue but can be also linked to a broad set of activities, including money laundering and corruption that negatively affect societies and needs a coordinated response.

The Standard enabled the automatic exchange of financial account information and has been designed in a standardised way to meet the needs of the jurisdictions and minimise the compliance burden on financial institutions to the extent possible.

The Global Forum on Transparency and Exchange of Information for Tax Purposes (the Global Forum) was called on by the G20 to monitor and review the implementation of this new global standard, including delivering a plan of action for developing countries' participation[2].

All jurisdictions, aside from the developing ones which do not host a financial centre, taking into account that they pose a lower risk to the level playing field and require a longer implementation period, were asked to commit to implement the CRS-AEOI standard by 2018. Nevertheless, all developing country members of the Global Forum are committed to implement the Standard within a practical timeframe.

1. OECD (2017), Standard for Automatic Exchange of Financial Account Information in Tax Matters, Second Edition, OECD Publishing, Paris, available at http://dx.doi.org/10.1787/9789264267992-en.

2. Global Forum / OECD (2017), The Global Forum's Plan of Action for Developing Countries Participation in AEOI, available at www.oecd.org/tax/transparency/documents/plan-of-action-AEOI-and-developing-countries.pdf.

Since September 2017, when the first exchanges took place, over 100 jurisdictions, including developed countries, major international financial centres and nine non-G20 developing countries[3] that do not host a financial centre, have commenced automatic exchanges.

With the delivery of its plan of action and the experience gained from the implementation of the Standard by monitoring and reviewing implementation as well as supporting developing countries, the Secretariat of the Global Forum has refined its approach and developed new capacity-building tools, including in the area of information security management. This renewed approach helped increase the participation of developing countries in CRS-AEOI, with 13 additional developing countries working closely with the Global Forum Secretariat and other development partners with a view to exchange by 2024.[4]

This toolkit aims to assist government officials from developing countries in the implementation of the CRS-AEOI standard and contains an introduction of the Standard, its key building blocks and an overview of the CRS-AEOI monitoring and peer review processes. It provides a hands-on implementation strategy to the Standard, and details the key considerations for jurisdictions when implementing the necessary international and domestic legal frameworks. It then gives an overview on how jurisdictions can ensure effective implementation, as well as details on how to ensure the effective use of data received from exchange partners. It contains examples of various approaches that have been taken by jurisdictions that have already implemented the Standard.

Each jurisdiction will have to carry out its own internal assessment of the most appropriate way to implement the Standard at a domestic level, taking into account the unique legal, policy and structural frameworks already in place, in recognition of the fact that there is no one-size-fits-all approach to achieving compliance with the international tax transparency standards.

A new strategy is being developed to support the participation of developing countries in the CRS-AEOI, which is a powerful tool to combat tax evasion and other illicit financial flows and to support their domestic resource mobilisation efforts. This toolkit is a structuring component of this ambitious strategy. It will continue to be updated over time, to capture further developments in relevant standards and best practices.

This toolkit was produced thanks to the generous support of donor countries and organisations, in particular the *Deutsche Gesellschaft für Internationale Zusammenarbeit* (GIZ) GmbH on behalf of German Federal Ministry for Economic Cooperation and Development (*Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung* – BMZ).

3. As of end September 2021: Albania, Azerbaijan, Colombia, Ecuador, Ghana, Malaysia, Nigeria, Pakistan and Peru.

4. The up-to-date status of CRS-AEOI commitments is available at www.oecd.org/tax/automatic-exchange/commitment-and-monitoring-process/AEOI-commitments.pdf.

About this toolkit

The aim of this toolkit is to assist developing countries that wish to implement the Standard for the automatic exchange of financial account information (CRS-AEOI standard or Standard) by providing practical guidance on the necessary steps to build a comprehensive implementation strategy and to have in place all the necessary building blocks to effectively participate in CRS-AEOI exchanges. This toolkit also provides guidance on critical post-implementation aspects, including ensuring effective implementation of the Standard and ensuring effective use of data, in line with the requirements of the Standard.

Many of the steps needed to implement the CRS-AEOI standard set out in the toolkit will lay the groundwork for the implementation of other types of tax information exchange should jurisdictions wish to pursue these in future, such as the automatic exchange of Country-by-Country Reports pursuant to Action 13 of the plan to address Base Erosion and Profit Shifting.[5]

The toolkit is divided into eight parts, as follows:

- Part 1 offers context on the CRS-AEOI standard by providing a brief history of the automatic exchange of information and an overview of the Standard itself. It outlines the benefits of becoming a Participating Jurisdiction.
- Part 2 provides an overview of the implementation of the Standard and its monitoring and review processes. It outlines the key building blocks necessary to implement the Standard, provides an overview of the due diligence requirements and present the relevant sources of information jurisdictions should refer to when implementing the Standard.
- Part 3 provides details on putting in place a strategy for implementation of the Standard: an important element to ensure that implementation is as smooth, timely and effective as possible. It presents the commitment process and provides a hands-on approach to develop and implement a sound strategy to meet the commitment made. It also details what support is offered by the Global Forum Secretariat during the implementation process and beyond.
- Part 4 provides guidance for jurisdictions that are considering the implementation of a voluntary disclosure programme in anticipation of the first CRS-AEOI exchanges.
- Part 5 presents an overview of the international legal framework, a key building block to allow the exchanges to take place, including details on the process to activate exchange relationships.
- Part 6 focuses on the domestic legal framework to implement the Standard. It covers the initial considerations when preparing domestic legislation and guidance, as well as details on each of the aspects of the Standard that must be included. It also includes details on each of the optional provisions where there is a policy decision for jurisdictions on whether to include them.
- Part 7 provides guidance on ensuring an effective implementation of the Standard, providing an overview on the putting in place of an administrative compliance framework. It also provides practical guidance on how to exchange information effectively, including details of how jurisdictions can put in place the technical systems needed to carry out the exchanges.
- Part 8 focuses on how jurisdictions can effectively use the data received from exchange partners, covering all phases of the process from the receipt of the data, on the treatment of the data, data matching and data analysis.

The Annexes contain a glossary of the main concepts covered in the toolkit, the substantive additional details to be reflected in the domestic legal framework, the model rules based on the "reference" method and useful resources.

5. OECD (2015), *Transfer Pricing Documentation and Country-by-Country Reporting, Action 13 - 2015 Final Report*, OECD/G20 Base Erosion and Profit Shifting Project, OECD Publishing, Paris, available at http://dx.doi.org/10.1787/9789264241480-en.

Capitalised terms used in this toolkit have a specific meaning and are defined in Section VIII of the Common Reporting Standard and / or in the glossary.

1. Introduction

Automatic exchange of information for tax purposes (AEOI) is an important tool available to tax authorities to administer and enforce their domestic tax legislation in a cross-border context.

The toolkit focuses on one specific form of AEOI provided in the international Standard for automatic exchange of financial account information (CRS-AEOI standard or Standard). It does not cover other forms of AEOI such as information exchanged under an Intergovernmental Agreement to Implement the Foreign Account Tax Compliance Act (FATCA IGA) or Country-by-Country Reporting (CbC reporting) information.

Section 1.1 presents the CRS-AEOI standard, explaining its origin and the background of its creation. It also gives an overview of the necessary requirements to implement the Standard domestically.

Section 1.2 focuses on the significant benefits of implementing the Standard. These include a significant boost to domestic revenue and taxpayer compliance, as well as improved transparency on financial flows investment. The implementation of the Standard also offers synergies with other tax transparency initiatives.

1.1. A NEW INTERNATIONAL STANDARD ON TRANSPARENCY AND EXCHANGE OF INFORMATION FOR TAX PURPOSES

AEOI refers to the exchange of a predefined set of information for tax purposes between competent authorities that takes place in a systematic manner, without any prior request.

Any information relevant for tax purposes can be subject to AEOI. For instance, some countries exchange information on income from employment, director's fees, and pensions on an automatic basis.

The CRS-AEOI standard requires the annual exchange of information on financial accounts held by individuals and entities resident in a foreign jurisdiction in a pre-defined format. The information exchanged includes details on the financial accounts and details on the account holder.

1.1.1. The history of automatic exchange of financial account information

As the world has become increasingly globalised, it is easier for taxpayers to make, hold and manage

investments through financial institutions outside their country of tax residence. Vast amounts of money is kept offshore and goes untaxed when taxpayers fail to comply with their tax obligations in the jurisdiction where they are tax resident. Offshore tax evasion is therefore a serious issue for all jurisdictions, small and large, developing and developed.

Jurisdictions have a shared interest in maintaining the integrity of their tax systems and need effective access to offshore information. Therefore, co-operation between tax authorities is critical in the fight against tax evasion and other illicit financial flows (IFFs). A key aspect of that co-operation is exchange of information (EOI) for tax purposes.

In 2014, the Organisation for Economic Co-operation and Development (OECD), mandated by the G20, developed the CRS-AEOI standard to facilitate cross-border tax transparency on financial accounts held abroad.[6]

All members of the Global Forum on Transparency and Exchange of Information for Tax Purposes (the Global Forum), aside from developing countries that did not host a financial centre, were asked to commit to automatically exchanging financial information under the CRS-AEOI standard by 2017 or 2018. Developing countries that do not host a financial centre were not called on to commit to the 2018 deadline in recognition of the lower risk they posed to the level playing field and the necessity of providing for a longer implementation period to accommodate capacity building.

This resulted in a group of 49 "early adopter" jurisdictions committing to exchanging information in 2017 and a further 51 jurisdictions committing to commencing exchanges in 2018. This coordinated implementation process has enabled the delivery of a level playing field, preventing taxpayers from moving their assets to non-committed jurisdictions in the attempt to avoid information sharing with the jurisdiction of their tax residence.

Since then, the number of committed jurisdictions has continued to increase. First, the impact of the implementation of the Standard on tax evasion and revenue mobilisation has convinced an increasing number of developing countries to take steps towards CRS-AEOI with the support of the Global Forum and other development partners. Second, the Global Forum has established a process to identify jurisdictions that have not implemented the Standard and pose a risk to its effectiveness. The jurisdictions found relevant for the implementation of the Standard are asked to commit to a specific date and are monitored by the Global Forum. Failing to commit or to meet the commitment can lead to negative outcomes for the concerned jurisdiction.

Currently, 120 jurisdictions are committed to exchange under the Standard by 2024 and further jurisdictions are likely to do so in the future.[7]

1.1.2. The basics of the standard on automatic exchange of financial account information

Under the CRS-AEOI standard, Financial Institutions report information to their domestic tax authorities on Financial Accounts held by foreign tax residents (individuals or Entities) and, in certain cases, held by Entities controlled by foreign tax residents (defined as Controlling Persons). Tax authorities then exchange that information with the tax authorities of the jurisdictions where the Account Holder and/or Controlling Persons are tax residents.

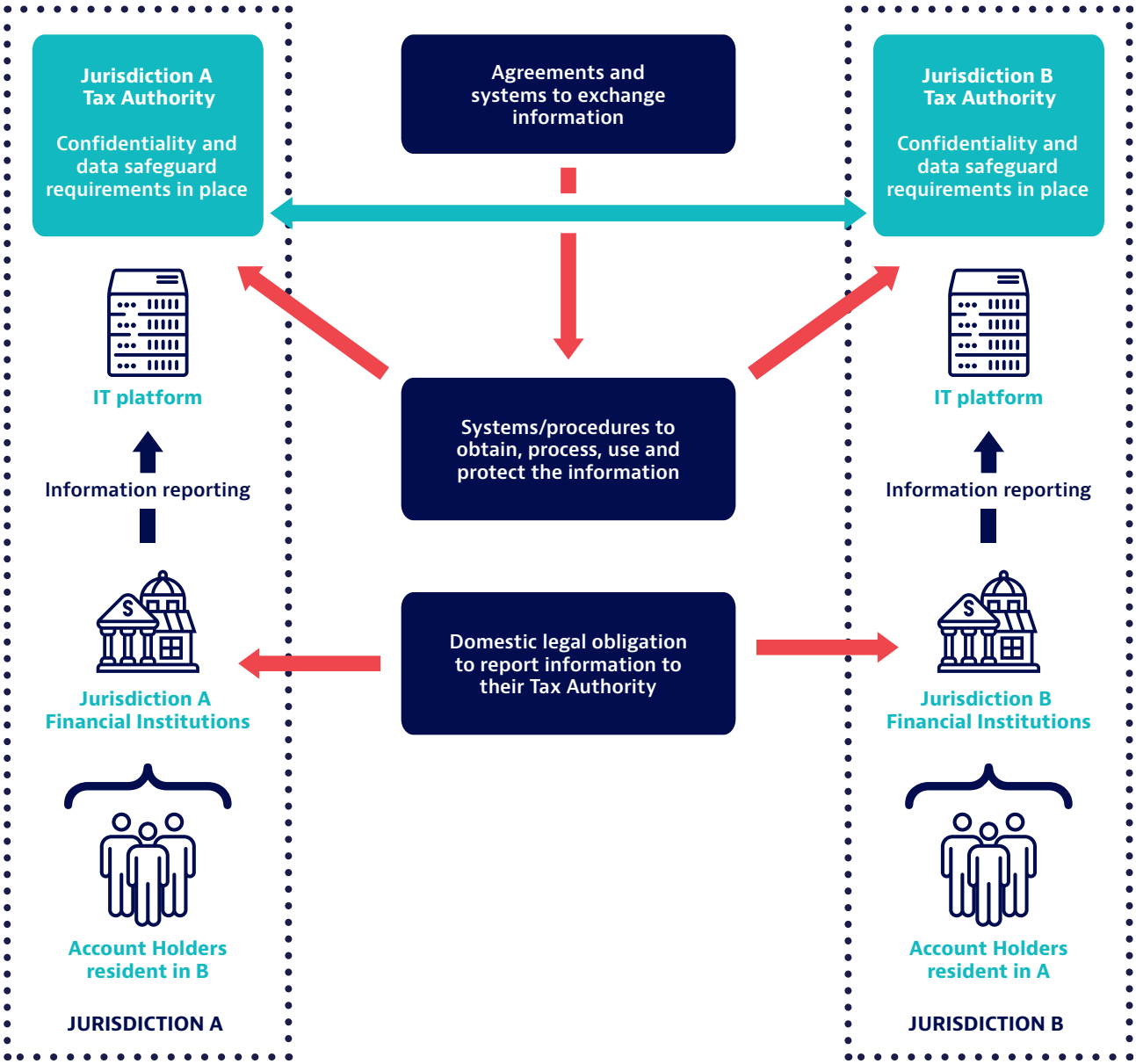
Figure 1 depicts the framework for reciprocal information exchange under the Standard, which requires:

- international agreements providing for CRS-AEOI exchange between the jurisdictions (i.e. an international legal basis)
- rules on the collection and reporting of information by Financial Institutions (i.e. a domestic legal basis)
- IT and administrative capabilities in order to receive and exchange the information
- measures to ensure the highest standards of confidentiality and data safeguards.

6. With a view to maximising efficiency and reducing cost for financial institutions, the CRS-AEOI standard draws extensively on FATCA IGA. The differences are driven by the multilateral nature of the standard and other aspects specific to the United States, in particular the concept of taxation on the basis of citizenship and the presence of a FATCA withholding tax. For more information on the differences with FATCA IGA, refer to §40-43 and §296-297 of the *Implementation Handbook* available at www.oecd.org/tax/exchange-of-tax-information/implementation-handbook-standard-for-automatic-exchange-of-financial-information-in-tax-matters.pdf.

7. The up-to-date list of jurisdictions committed to start CRS-AEOI by a specific date is available at www.oecd.org/tax/automatic-exchange/commitment-and-monitoring-process/AEOI-commitments.pdf.

FIGURE 1. **Overview of the framework for automatic exchange of financial account information**



1.2. BENEFITS OF IMPLEMENTING THE STANDARD ON AUTOMATIC EXCHANGE OF FINANCIAL ACCOUNT INFORMATION

Transparency is at the heart of the fight against tax evasion and other IFFs. Although all jurisdictions suffer from these practices, this problem is often especially acute in developing countries, particularly when tax administrations have capacity constraints to enforce tax and other laws in a cross-border context.

Developing countries are disproportionately exposed to the risks of international tax evasion and therefore their need for access to the world's information exchange systems is proportionately greater. By not participating in CRS-AEOI, developing countries risk losing out in their fight against tax evasion and other IFFs. Conversely, by being part of the global move towards greater tax transparency, they stand to gain the most by generating additional tax revenues, which are of critical importance for delivering the vital public services and meeting the sustainable development goals.

With access to the most advanced EOI tools, developing countries can significantly strengthen their tax enforcement units, generate additional revenues, and strengthen the level of public trust in the tax system. CRS-AEOI is a very powerful tool which gives tax authorities visibility over the foreign accounts of their residents, making it far more difficult for tax evaders to hide assets and income abroad. Tax authorities can use the information exchanged under the Standard to verify whether taxpayers are properly declaring their international financial affairs and paying the tax that is due to their domestic tax authorities. This is important to tackle tax evasion as well as to maintain public confidence that the increasing globalisation of the financial system is not undermining domestic tax systems.

1.2.1. Significant boost to domestic revenue and taxpayer compliance

The impact of the emergence of this international standard has been felt in the jurisdictions which committed to implement it, even before any exchanges occurred. At least EUR 65 billion in additional revenue (tax, interest, and penalties) have been identified worldwide in the 2014-20 period through voluntary disclosure programmes (VDPs) launched prior to the first exchanges (of which EUR 25 billion for developing countries). In addition, since 2017, the use of exchanged data has already helped deliver at least EUR 3 billion of additional tax revenues globally (EUR 500 million for developing countries).

With millions of taxpayers having come forward to tax authorities to declare income and gains through VDPs,[8] the implementation of the CRS-AEOI standard should result in a long-term increase in domestic revenue as these taxpayers continue to comply with their tax obligations. In addition, a number of taxpayers also started to spontaneously declare foreign assets or incomes that they were not reporting in previous years, which will lead to additional revenues for the future, and to investigations into potential non-compliance in the past.

The Standard has also contributed to a significant increase in the number of taxpayers registered with their tax authority in some countries. For instance, Nigeria reported that the number of taxpayers registered in its systems grew from 14 million in 2016 to 19 million in 2019 in the context of its VDP.[9]

With the massive amount of financial account data received by tax authorities, potential cases of non-compliance are identified and investigated. In that context, requests for additional information have been made by many jurisdictions for specific cases. In certain instances, group requests[10] were also made in accordance with the Standard on transparency and exchange of information on request (EOIR standard). This shows how the CRS-AEOI and EOIR standards are complementary and mutually reinforcing in delivering greater transparency.

1.2.2. Improved transparency on financial flows investment

In 2020, 101 jurisdictions automatically exchanged information on at least of 75 million financial accounts worldwide, covering total assets of nearly EUR 9 trillion.[11] In 2021, 109 jurisdictions are due to exchange information based on a network of exchange relationships that has increased by 7% over the previous year, to around 7 500.

With increased transparency on financial accounts held abroad, the implementation of the Standard has already led to a change in the behaviours of tax evaders. Studies have shown a correlation between the commencement of CRS-AEOI in 2017 and 2018 and a significant decrease (-22%) in foreign-owned bank deposits in international financial centres (IFCs), which has coincided with an increase deposits in non-IFCs.[12] There is also evidence that the number of foreign financial accounts and the income from these accounts reported to tax authorities increased significantly.

8. Global Forum / OECD (2020), *Tax Transparency and Exchange of Information in Times of COVID-19, 2020 Global Forum Annual Report*, available at www.oecd.org/tax/transparency/documents/global-forum-annual-report-2020.pdf.

9. Global Forum Secretariat / OECD (2019), *Tax Transparency in Africa, Africa Initiative Progress Report 2018*, available at www.oecd.org/tax/transparency/documents/africa-initiative-report-2018.pdf.

10. A group request is a request for information on a group of taxpayers who are not individually identified.

11. OECD (2021), *OECD Secretary-General Tax Report to G20 Finance Ministers and Central Bank Governors, Italy, October 2021*, op. cit.

12. O'Reilly P., Ramirez K.P. and Stemmer M.A. (2019), *Exchange of Information and Bank Deposits in International Financial Centres*, OECD Taxation Working Papers, No. 46, OECD Publishing, Paris, available at https://doi.org/10.1787/025bfebe-en.

In addition to an increase in revenues, improving transparency for tax purposes reduces a jurisdiction's exposure to all forms of IFFs. Certain requirements of the CRS-AEOI standard overlap with the Financial Action Task Force (FATF) Recommendations on anti-money laundering and counter financing of terrorism (AML/CFT). For instance, the identification in certain cases of the beneficial owners of Entities holding Financial Accounts (defined as Controlling Persons in CRS-AEOI) corresponds to the FATF Recommendations. Consequently, the Standard requires compliance with key elements of the FATF Recommendations as well as an effective enforcement and supervision of the implementation of the obligations by Financial Institutions. More generally, unveiling the legal and beneficial ownership structures of Entities (i.e. legal persons and arrangements) that hold Financial Accounts also assists the law enforcement authorities in preventing or detecting the misuse of legal persons and arrangements for corruption, money laundering and other financial crimes.

Finally, in accordance with treaty provisions and subject to prior authorisation from the sending jurisdiction, jurisdictions are able to use specific data collected through exchange of information for purposes other than tax (e.g. to tackle corruption or money laundering).

1.2.3. Synergies with other tax transparency initiatives

Although the initial investment in the implementation of the CRS-AEOI standard and associated compliance costs may appear significant, in addition to the immediate benefits described above, the medium to long-term return is potentially even higher. This is thanks not only to the possibility of using CRS-AEOI data for tax enforcement purposes (i.e. from tax assessment to tax collection), but also to the significant deterrent effect associated with the availability of offshore financial account information domestically.

There are also synergies in implementing the Standard with other forms of automatic or mandatory spontaneous exchange which further enhance potential revenue gains:

- country-by-country reporting[13]
- mandatory disclosure rules[14]
- reporting by digital platforms[15]
- exchange on tax rulings.[16]

The CRS-AEOI standard shares some of the key building blocks with these other exchanges, such as an international legal basis allowing for exchange of information, an appropriate confidentiality and data safeguards framework, administrative and IT capacity and a secure system to transmit the data with exchange partners.

Therefore, a jurisdiction may wish to take advantage of the implementation of the Standard to simultaneously implement other forms of exchange. It may also wish to consider the potential implementation of these other forms of exchange at a later stage when implementing key building blocks, in particular when developing the IT infrastructure.

13. OECD (2015), *Transfer Pricing Documentation and Country-by-Country Reporting*, Action 13, op. cit.

14. OECD (2015), *Mandatory Disclosure Rules*, Action 12 - 2015 Final Report, OECD/G20 Base Erosion and Profit Shifting Project, OECD Publishing, Paris, available at http://dx.doi.org/10.1787/9789264241442-en.

15. OECD (2021), *Model Reporting Rules for Digital Platforms: International Exchange Framework and Optional Module for Sale of Goods*, OECD, Paris, available at www.oecd.org/tax/exchange-of-tax-information/model-reporting-rules-for-digital-platforms-international-exchange-framework-and-optional-module-for-sale-of-goods.pdf and OECD (2020), *Model Rules for Reporting by Platform Operators with respect to Sellers in the Sharing and Gig Economy*, OECD, Paris, available at www.oecd.org/tax/exchange-of-tax-information/model-rules-for-reporting-by-platform-operators-with-respect-to-sellers-in-the-sharing-and-gig-economy.htm.

16. OECD (2015), *Countering Harmful Tax Practices More Effectively, Taking into Account Transparency and Substance*, Action 5 - 2015 Final Report, OECD/G20 Base Erosion and Profit Shifting Project, OECD Publishing, Paris, available at http://dx.doi.org/10.1787/9789264241190-en.

2. Overview of the implementation of the standard and its monitoring and assessment framework

The implementation of the Standard was particularly challenging for the "early adopters" as it was a new standard with very specific requirements to ensure it can work in a multilateral context. Although the implementation process will vary depending on each jurisdiction's unique circumstances, the main elements of the Standard are intended to result in uniform implementation across jurisdictions. This ensures a level playing field and minimises the burden for Financial Institutions and tax authorities, as well as best supporting the effective use of the information.

Section 2.1 presents reference documents and tools relevant to the implementation of the Standard.

This implementation is based on three main building blocks, which are critical to its proper functioning. While an overview of these building blocks is provided in Section 2.2, further detailed guidance on each of them is provided in the following parts of the toolkit. A high-level description of the Common Reporting Standard is provided in Section 2.3.

In order to maintain the level playing field and ensure the integrity of the CRS-AEOI system so that tax evaders cannot hide their financial assets, all committed jurisdictions are subject to a monitoring process during the implementation of the Standard and a peer review process to assess whether they have correctly implemented all elements of the Standard. An overview of the monitoring and peer review process is provided in Section 2.4.

2.1. REFERENCE DOCUMENTS AND TOOLS FOR THE IMPLEMENTATION OF THE STANDARD

Various documents have been produced to support the implementation of the CRS-AEOI standard.

The main documents which jurisdictions should refer to when implementing the Standard are:

- the CRS-AEOI standard itself
- the Implementation Handbook
- the CRS-AEOI related Frequently Asked Questions (FAQs)
- the Guide on Promoting and Assessing Compliance by Financial Institutions.

These documents are further described in the subsections below.

2.1.1. The standard for Automatic Exchange of Financial Account Information in Tax Matters

The CRS-AEOI standard[17] is composed of four main components:

- a Model Competent Authority Agreement (CAA)
- the Common Reporting Standard (CRS)
- the Commentaries on the CAA and the CRS
- the CRS extensible mark-up language (XML) Schemas and related User Guides.

Table 1 unpacks the Standard.

2.1.2. The Implementation Handbook

The Implementation Handbook[18] aims to assist government officials when implementing the CRS-AEOI standard. It also provides a practical overview of the Standard to both the financial sector and the public at-large, including an overview of legislative, technical and operational issues.

2.1.3. The Common Reporting Standard related Frequently Asked Questions

The OECD maintains and regularly updates a list of frequently asked questions on the application of the CRS.[19] These FAQs were received from business and government delegates. The answers to such questions provide further precision on the CRS and help to ensure consistency in implementation.

These FAQS are generally interpretive in nature and draw upon existing foundations in the Standard or its Commentary. As such, it is expected that most jurisdictions would readily be able to apply the conclusions found in the FAQs without explicitly incorporating these in the legal framework.

2.1.4. The Guide on Promoting and Assessing Compliance by Financial Institutions

The Guide on Promoting and Assessing Compliance by Financial Institutions[20] was released by the OECD Forum on Tax Administration (FTA) to assist government officials and Financial Institutions regarding their obligations to monitor and to ensure compliance with the reporting obligations under the CRS and FATCA.

The guide provides an overview on the various necessary elements that a compliance framework should include, outlining strategies and initiatives that tax authorities might want to pursue to promote and support compliance by Financial Institutions. It also provides in-depth details on compliance assessments, focusing on the key areas of governance and implementation, due diligence obligations and reporting requirements. The guide includes example questions on these key areas that tax authorities could use to determine whether Financial Institutions have fulfilled the necessary reporting and due diligence obligations. The guide is not intended to be prescriptive but instead presents some of the approaches that jurisdictions can adopt. An overview on the administrative compliance frameworks jurisdictions will need to have in place is provided in Section 7.1 of this toolkit.

2.1.5. The Automatic Exchange Portal

The Automatic Exchange Portal[21] provides a comprehensive overview of the work of the OECD and the Global Forum in the AEOI area, in particular with respect to CRS-AEOI, which can be helpful when implementing the Standard. This includes:

- the reference documents mentioned above are made available on the website
- relevant information on the international framework, including the list of CRS MCAA signatories and the activated bilateral relationships for the exchange of CRS information

17. OECD (2017), *Standard for Automatic Exchange of Financial Account Information in Tax Matters, op. cit.*
18. OECD (2018), *Standard for Automatic Exchange of Financial Information in Tax Matters - Implementation Handbook* – Second Edition, OECD, Paris available at www.oecd.org/tax/exchange-of-tax-information/implementation-handbook-standard-for-automatic-exchange-of-financial-account-information-in-tax-matters.htm.
19. CRS-related FAQs are available at: www.oecd.org/tax/automatic-exchange/common-reporting-standard/CRS-related-FAQs.pdf.
20. OECD (2020), *Automatic Exchange of Information: Guide on Promoting and Assessing Compliance by Financial Institutions*, Paris. Available at www.oecd.org/tax/forum-on-tax-administration/publications-and-products/automatic-exchange-of-information-guide-on-promoting-and-assessing-compliance-by-financial-institutions.htm.
21. Accessible at www.oecd.org/tax/automatic-exchange/.

Overview of the implementation of the standard and its monitoring and assessment framework

Table 1. **The CRS-AEOI standard unpacked**

<table>
<tr><th>Component</th><th>Purpose</th></tr>
<tr><td>The Model CAA</td><td>The Model CAA is a bilateral agreement that can be signed by competent authorities to supplement their existing international agreement providing for automatic exchange of financial account information. The Model CAA provides for the information to be identified in accordance with the CRS and exchanged by the partners, the timing and modalities of the exchanges, as well as requirements to ensure the confidentiality and safeguarding of the data (CRS-AEOI standard, Part II B).

The Standard also contains a:

● multilateral model CAA (CRS-AEOI standard, Annex 1)

● non-reciprocal model CAA (CRS-AEOI standard, Annex 2).

While the Standard allows for bilateral CAAs, the jurisdictions implementing the Standard have signed and activated the Multilateral Competent Authority Agreement on Automatic Exchange of Financial Account Information (CRS MCAA) which supplements Article 6 of the Convention on mutual Administrative Assistance in Tax Matters (MAAC) (see Part 5 of the toolkit).</td></tr>
<tr><td>CRS</td><td>The CRS is a common set of due diligence and reporting requirements that Financial Institutions must follow as well as measures jurisdictions will have to have in place to ensure effective implementation. This common set of requirements ensures the quality and predictability of the information exchanged (CRS-AEOI standard, Part II B). It forms the core element of the Standard. An overview of the nine sections of the CRS is provided below (see also Subsection 2.3 of the toolkit).

<table><tr><th>CRS Section</th><th>Content</th></tr><tr><td>Section I</td><td>General Reporting Requirements</td></tr><tr><td>Section II</td><td>General Due Diligence Requirements</td></tr><tr><td>Section III</td><td>Due Diligence for Preexisting Individual Accounts</td></tr><tr><td>Section IV</td><td>Due Diligence for New Individual Accounts</td></tr><tr><td>Section V</td><td>Due Diligence for Preexisting Entity Accounts</td></tr><tr><td>Section VI</td><td>Due Diligence for New Entity Accounts</td></tr><tr><td>Section VII</td><td>Special Due Diligence Rules</td></tr><tr><td>Section VIII</td><td>Defined Terms</td></tr><tr><td>Section IX</td><td>Effective Implementation</td></tr></table>
A wider approach of the CRS to facilitate the implementation in a global context is also available in Annex 5 of the CRS-AEOI standard. This allows Financial Institutions to carry out the due diligence processes across all of the Financial Accounts they maintain, even if not all of the information is required to be reported immediately, supporting an efficient implementation.</td></tr>
<tr><td>The Commentaries to the CAA and the CRS</td><td>For each section of the CAA and the CRS, detailed Commentaries provide additional detail and interpretational guidance. The Commentaries contain substantial guidance to be followed by implementing jurisdictions. This is are essential to ensure consistency and uniform implementation across jurisdictions and to avoid unnecessary costs and complexity for Financial Institutions (CRS-AEOI standard, Part III).</td></tr>
</table>

Component	Purpose
The CRS XML schemas and User Guides	The CRS XML Schema is the IT-based and standardised format for the exchange of information under the Standard.[22] The related User Guide explains the information required to be included in each data element to be reported in the CRS XML Schema. It should be noted that, since 1 February 2021, the User Guide in Annex 3 of the Standard has been replaced by version 2.0 of the CRS XML Schema. The CRS XML Schema User Guide for Tax Administrations (version 3.0) has been updated accordingly.[23] In addition, a standardised IT-format for providing structured feedback on exchanged CRS information – the CRS Status Message XML Schema[24] – as well as a related User Guide have been published.[25] More information is provided in Section 7.2 of this toolkit.

- information to assist government authorities, Financial Institutions and taxpayers in applying the Standard correctly, including:
  - a comprehensive overview of the legislation, regulations and guidance that jurisdictions have developed for the purpose of implementing the CRS
  - information on jurisdictions' Tax Identification Numbers (TINs) and tax residency rules, which can be referred to by Financial Institutions when implementing the requirements
  - guidance for Financial Institutions on how to carry out their CRS due diligence obligations in relation to high-risk Residence and Citizenship by Investment Schemes
  - a sample of self-certification forms[26] drafted by the Business and Industry Advisory Committee to the OECD (BIAC)[27]
- the status of the commitments made, the outcome of the monitoring of their delivery and the peer review.

2.2. KEY BUILDING BLOCKS FOR THE IMPLEMENTATION OF THE STANDARD ON AUTOMATIC EXCHANGE OF FINANCIAL ACCOUNT INFORMATION

The CRS-AEOI standard requires the annual exchange of information on Financial Accounts held by foreign tax residents (individuals or Entities) and those held by Entities controlled by foreign tax residents (defined as Controlling Persons). Tax authorities then exchange that information with the tax authorities of the jurisdictions where the Account Holder and/or Controlling Persons are tax resident in a pre-defined format. The information exchanged includes details on the Financial Accounts, the Reporting Financial Institution and the Account Holder and/or Controlling Persons.

In practice, jurisdictions need to put in place three key building blocks to implement the Standard. These building blocks are:

- an international and domestic legal framework
- administrative and IT resources
- an appropriate confidentiality and data safeguards framework.

The steps to be taken to implement these building blocks can be done in any order or can be pursued in parallel (see also Part 3 of this toolkit).

22. The CRS XML Schema Version 2.0 is available at www.oecd.org/tax/automatic-exchange/common-reporting-standard/schema-and-user-guide.
23. OECD (2019), *Common Reporting Standard XML Schema: User Guide for Tax Administrations*, Version 3.0 – June 2019, OECD, Paris, available at www.oecd.org/tax/exchange-of-tax-information/common-reporting-standard-xml-schema-user-guide-for-tax-administrationsjune-2019.pdf.
24. The CRS Status Message XML Schema Version 2.0 is available at www.oecd.org/tax/exchange-of-tax-information/common-reporting-standard-status-message-xml-schema-user-guide-for-tax-administrations.htm.
25. OECD (2019), *Common Reporting Standard Status Message XML Schema: User Guide for Tax Administrations*, Version 2.0 – June 2019, OECD, Paris, available at www.oecd.org/tax/exchange-of-tax-information/common-reporting-standard-status-message-xml-schema-user-guide-for-tax-administrations-june-2019.pdf.
26. The OECD has not approved the forms and neither the OECD nor BIAC regard them as mandatory or as best practice documents.
27. BIAC is an independent international business association devoted to giving the OECD business perspectives on a broad range of global policy issues.

2.2.1. Legislative framework

Domestic legal framework

In order to implement the Standard, jurisdictions need to translate the reporting and due diligence requirements provided in the CRS into domestic law. These requirements set out which Financial Institutions are required to report, the accounts they need to report on and the information to be reported.

This standardised set of rules for Financial Institutions, set out in the CRS and its Commentary, ensure consistency in the scope and quality of information exchanged.

Furthermore, jurisdictions must also put in place a number of provisions to ensure that the Standard is implemented effectively. Detailed guidance is provided in Part 6 of this toolkit.

International legal framework

The implementation of the Standard requires an international legal basis that provides for AEOI between jurisdictions. Whilst bilateral treaties, such as those based on Article 26 of the OECD Model Tax Convention[28], permit such exchanges, all implementing jurisdictions have established relationships through a multilateral instrument, such as the Convention on Mutual Administrative Assistance in Tax Matters (MAAC).[29]

In addition to these instruments, the competent authorities of the jurisdictions must define in advance the scope of information to be exchanged, in accordance with the Standard. Therefore, in order to implement the Standard, a CAA is required to activate and operationalise the CRS-AEOI relationship between jurisdictions and which specifies what information will be exchanged and when. A Multilateral Competent Authority Agreement on Automatic Exchange of Financial Account Information[30] (CRS MCAA) was developed to facilitate the large-scale implementation of the CRS-AEOI standard.

Taking into account the commitment of jurisdictions to perform CRS-AEOI with all Interested Appropriate Partners,[31] implementing jurisdictions have established their CRS-AEOI relationships using the MAAC and the CRS MCAA. Detailed guidance is provided in Part 4 of this toolkit.

2.2.2. Administrative and IT capacity

In addition to having a legislative framework in place, tax administrations also need technical and administrative resource to perform exchanges in accordance with the CRS-AEOI standard. Both technical and human resource will be needed to:

- **Receive the information from Financial Institutions:** a system must be put in place to allow Financial Institutions to submit the required information to the tax authority, such as through a government AEOI portal (see Section 7.2 of the toolkit).
- **Send and receive information with exchange partners:** the methods of encryption and transmission of the CRS data shall be agreed upon by the exchange partners. In order to ensure an efficient, secure and timely means to transmit the CRS data, the FTA designed and built the Common Transmission System (CTS). The CTS is a secure and encrypted "pipe", incorporating the latest IT-security standards, through which competent authorities of the partner jurisdictions can send and/or receive CRS information (see Section 7.2 of the toolkit). This is the transmission system used for CRS-AEOI exchanges by all jurisdictions that have implemented the standard to date.
- **Ensure compliance with due diligence and reporting obligations:** in order to ensure effective implementation of the CRS-AEOI standard in practice, a comprehensive administrative compliance framework must be put in place to ensure that Financial Institutions implement the requirements effectively in practice (see Section 7.1 of the toolkit).
- **Use the CRS data received:** the ultimate goal of the implementation of the Standard is to ensure transparency over offshore Financial Accounts. Receiving jurisdictions therefore use the information exchanged to ensure tax compliance, enforce their tax laws, collect unpaid taxes, and, more generally, tackle tax evasion and other IFFs (see Part 8 of the toolkit).

28. OECD (2017), *Model Tax Convention on Income and on Capital: Condensed Version 2017*, OECD Publishing, available at http://dx.doi.org/10.1787/mtc_cond-2017-en.

29. OECD and Council of Europe (2011), *The Multilateral Convention on Mutual Administrative Assistance in Tax Matters: Amended by the 2010 Protocol*, OECD Publishing, available at http://dx.doi.org/10.1787/9789264115606-en.

30. The text of the CRS MCAA is available at www.oecd.org/tax/automatic-exchange/international-framework-for-the-crs/multilateral-competent-authority-agreement.pdf.

31. An Interested Appropriate Partner is any jurisdiction that wants to receive information from a committed jurisdiction and that meets the expected standards in relation to confidentiality and data safeguards.

These considerations should be taken into account early in the implementation process to ensure adequate resources are put in place by the time of exchange.

2.2.3. Confidentiality and data safeguards

Information confidentiality and security is essential to the relationship between tax authorities and taxpayers. The confidentiality of taxpayer information is therefore a fundamental cornerstone of all exchanges of tax information. The CRS-AEOI standard requires jurisdictions to have appropriate confidentiality and data safeguards in place. This should translate into a legal framework ensuring the confidentiality and appropriate use of exchanged information, an information security management framework that adheres to internationally recognised standards or best practices, and enforcement provisions and processes to address confidentiality breaches. These considerations also derive from the international agreements that facilitate CRS-AEOI exchanges.

The Confidentiality and Information Security Management Toolkit[32] provides detailed guidance to support jurisdictions in implementing appropriate confidentiality and data safeguards.

2.3. HIGH-LEVEL ARCHITECTURE OF THE COMMON REPORTING STANDARD

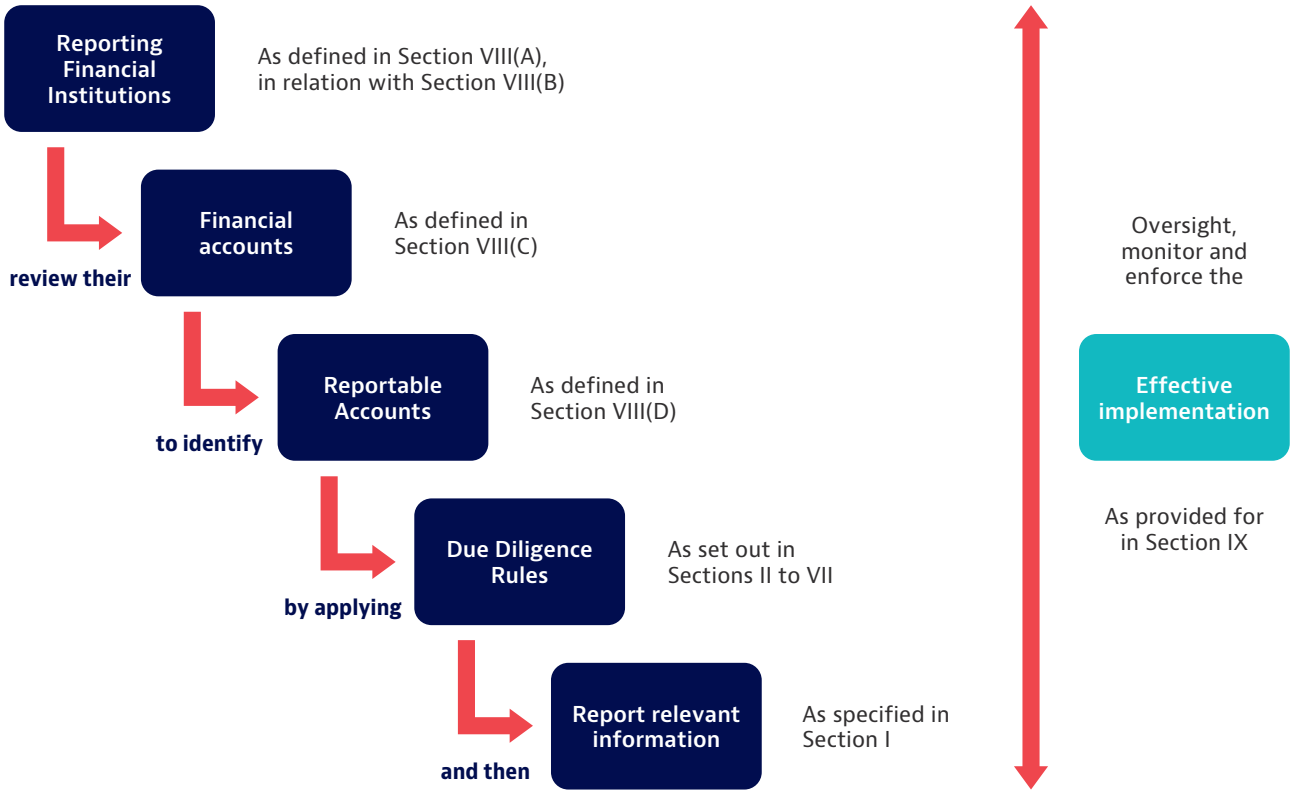
The CRS requires Reporting Financial Institutions to review their Financial Accounts to identify Reportable Accounts by applying due diligence rules and then report the relevant information to the competent authority. This process will need to be implemented effectively by jurisdictions.

The CRS is divided into nine sections:

- Section I specifies the information to be reported.
- Sections II to VII sets out the due diligence rules.

32. Global Forum Secretariat / OECD (2020), *Confidentiality and Information Security Management Toolkit*, available at www.oecd.org/tax/transparency/documents/confidentiality-ism-toolkit_en.pdf.

FIGURE 2. **Overview of the Common Reporting Standard**



- Section VIII provides the relevant definitions, including for Reporting Financial Institution, Financial Account and Reportable Account.
- Section IX sets out how jurisdictions should ensure the effective implementation of the Standard.

Figure 2 provides an overview of the CRS.

The purpose of the following sections is only to provide an overview of the CRS. The CRS and its Commentary provide the full description of the CRS requirements.

2.3.1. The scope of the Common Reporting Standard

Section VIII of the CRS provides for the relevant definitions to implement the CRS, including (i) Reporting Financial Institution, (ii) Financial Account and (iii) Reportable Account.

Reporting Financial Institutions are required to carry out due diligence procedures and report the relevant information under the CRS. A Reporting Financial Institution is a Financial Institution (i.e. Depository Institution (e.g. banks), Custodial Institution (e.g. brokers), Investment Entities (e.g. funds), Specified Insurance Companies (e.g. life insurance companies) that are not otherwise exempted from these obligations for being considered as low risks (i.e. Non-Reporting Financial Institutions).

Figure 3 illustrates the process for determining if an Entity is a Reporting Financial Institution.

Financial Accounts are what Reporting Financial Institution must review. A Financial Account is a an account maintained by a Financial Institution that is not otherwise excluded for being considered as low risk (i.e. Excluded Accounts). A Financial Account can be a Depository Account (e.g. debt, checking or savings account), a Custodial Account (i.e. where a financial asset such as a share of a corporation is held in custody for the benefit of the account holder), an Equity or Debt Interest in an Investment Entity (e.g. participation in a fund), a Cash Value Insurance Contract or Annuity Contracts (e.g. an insurance contract with a cash value or investment component).

FIGURE 3. **Reporting Financial Institutions**

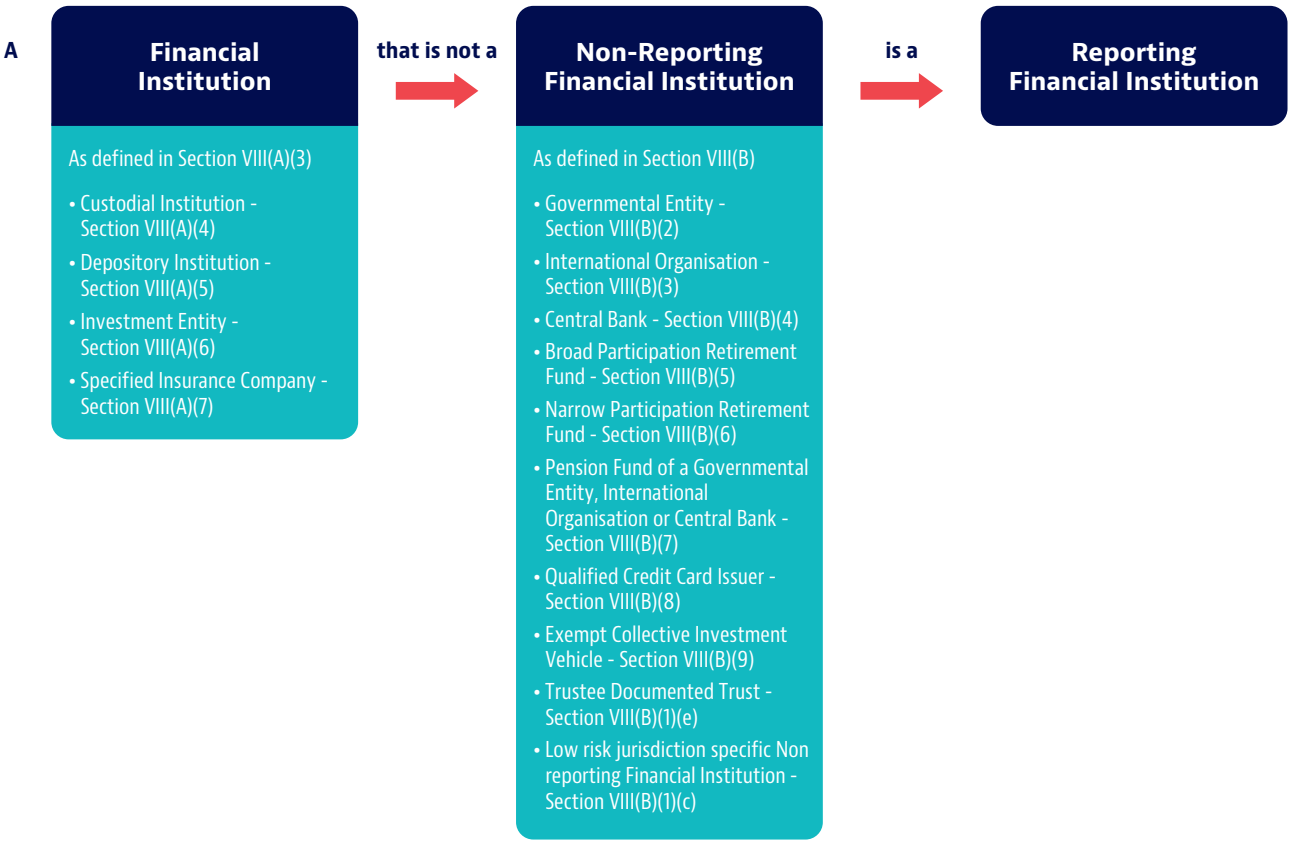


Figure 4 illustrates the process for determining if an account is a Financial Account. The terms Financial Account and Excluded Accounts are defined in Section VIII(C) of the CRS.

Reportable Accounts are the accounts for which information must be reported. A Reportable Account is a Financial Account that, as a consequence of the due diligence procedures, is:

a. identified as being held by:

   (i) a Reportable Jurisdiction Person, i.e. an Individual or Entity that is a tax resident in a partner jurisdiction, and/or

   (ii) a Passive Non-Financial Entity (NFE) (such as shell entities or certain entities generating passive income, e.g. dividends and interest, and holding assets that generates passive income) with one or more Controlling Persons, such as individuals with a beneficial ownership interest in the Entity, that is or are a tax resident in a partner jurisdiction, and

b. that is not excluded from being reported for being considered low risk, such as corporations the stock of which is publicly traded and its related entities.

Figure 5 illustrates the process for determining if a Financial Account is a Reportable Account. The terms Reportable Account, Reportable Jurisdiction Person, Reportable Person, Reportable Jurisdiction (i.e. partner jurisdiction), Passive NFE and Controlling Person are defined in Section VIII(D) of the CRS.

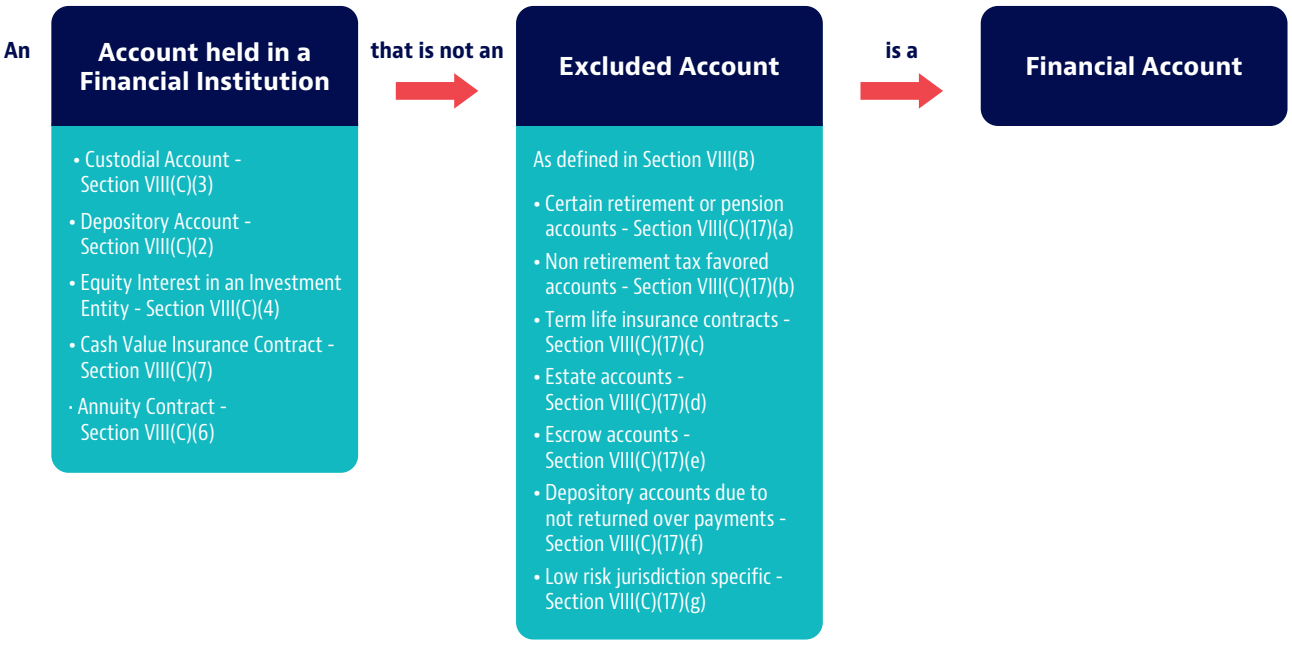
2.3.2. The due diligence procedures

The due diligence is the set of actions and procedures that Reporting Financial Institutions must carry out with respect to Financial Accounts in order to identify the Reportable Accounts. The CRS due diligence rules are in addition to the AML/KYC procedures although they may partly rely on AML/KYC procedures in some cases. Table 2 summarises the main due diligence procedures of Section III to VII of the CRS.

Additionally, Sections II and VII of the CRS lays out General Due Diligence Requirements and Special Due Diligence Rules respectively, that are applicable to any type of Financial Account, e.g. the standard to rely on a self-certification, as well as the account balance aggregation and currency rules.

Figure 6 summarises the architecture of the due diligence rules for Individual Accounts and Entity Accounts.

FIGURE 4. **Financial Accounts**



2.3.3. Information to be reported

Once a Reporting Financial Institution has identified a Reportable Account, it shall report the required information to its tax authority. Such information is specified in Section I of the CRS:

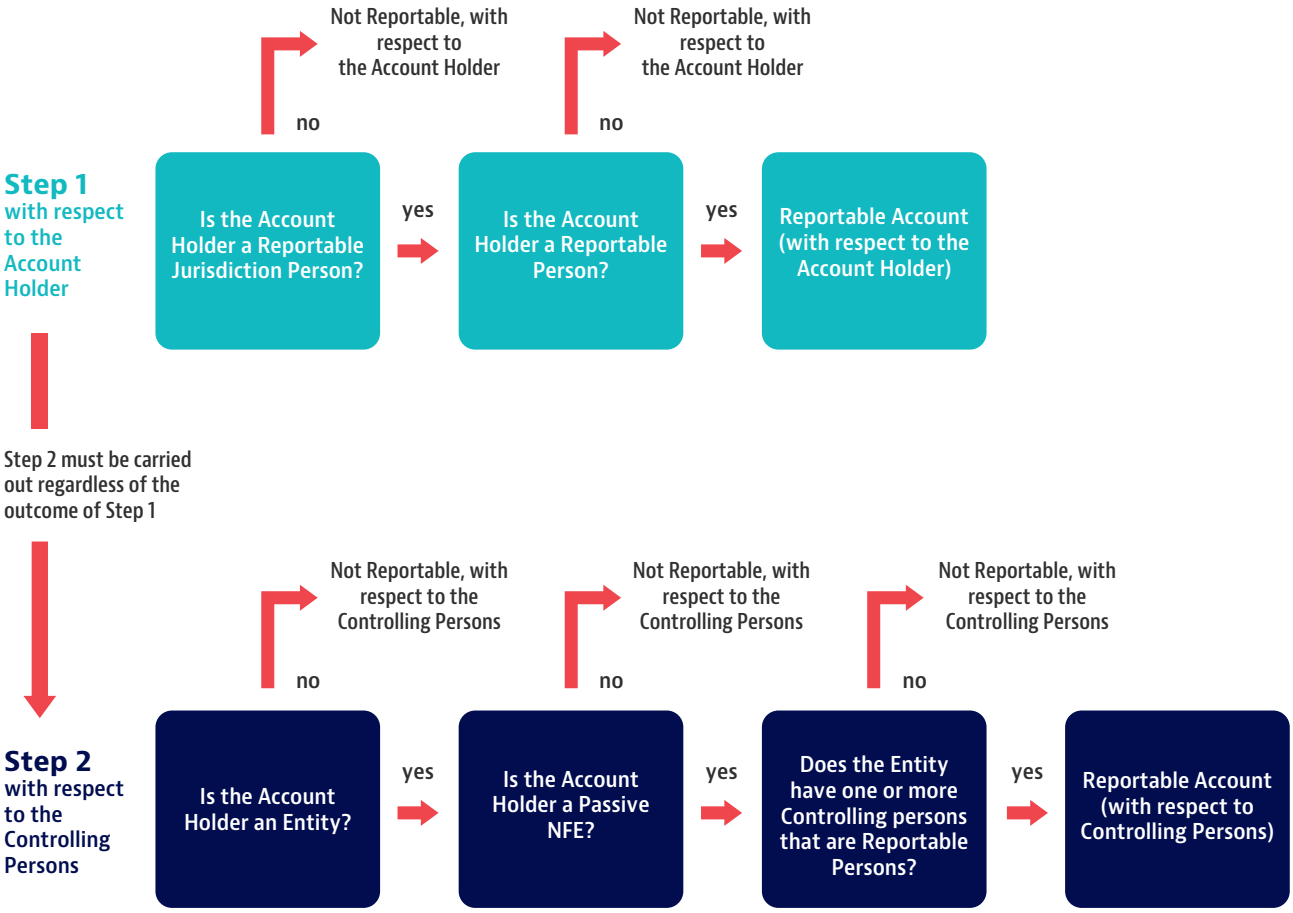
- identification of Account Holders or Controlling Persons
  - name, address, jurisdiction of residency, TIN, date and place of birth of the Account Holder and, if applicable, of the Controlling Persons
- Identification of the Financial Account
  - account number
  - name of the Financial institution and identification number (such as the Global Intermediary Identification Number (GIIN))
- financial information
  - balance or value of the account or, if the account was closed, the fact of the closure of the account
  - payments made to the account by the Financial Institution, such as the total gross amount of interest and dividends, as well as the total gross proceeds from the sale or redemption of financial assets held in the account and other payments made to the account by the Financial Institution.

Table 2. **Summary of the CRS due diligence**

<table>
<tr><th colspan="3">Type of Financial Accounts</th><th>Summary of the due diligence</th></tr>
<tr><td rowspan="3">Individual Accounts
(i.e. accounts held by natural persons).
Section III and IV.</td><td rowspan="2">Preexisting Accounts
(i.e. as defined by domestic legislation – typically accounts opened prior the date of effect of the legislation implementing the CRS).
Section III.</td><td>Lower Value Accounts
(i.e. with a balance or value equal to or less than USD 1 million).
Section III(B).</td><td>The Reporting Financial Institution may either:
i. rely on the residence address test, i.e. considering that the Account Holder is resident for tax purposes in the jurisdiction they have registered as their residence address in the records of the Financial Institution, to the extent that such residence address is supported by documentary evidence (e.g. identity card) (optional – see Subsection 6.3.10 of the toolkit). Section III(B)(1).
ii. search for indicia (e.g. residence address, telephone number) of tax residency on its electronically searchable database. Section III(B)(2).</td></tr>
<tr><td>High Value Accounts
(i.e. with a balance or value above USD 1 million).
Section III(C).</td><td>The Reporting Financial Institution cannot rely on the residence address test and shall always look for indicia on its electronically searchable database and, if applicable, in its paper records or after consulting with the relationship manager (i.e. the employee of the bank in charge of the account).</td></tr>
<tr><td colspan="2">New Accounts
(i.e. as defined by domestic legislation – typically accounts opened on or after the date of effect of the legislation implementing the CRS).
Section IV.</td><td>The Reporting Financial Institution shall always:
i. obtain a valid self-certification (i.e. it contains at least, the name, residence address, jurisdiction of tax residency, date of birth of the Account Holder and a TIN for each Reportable Jurisdiction if the individual has been issued such a number)
ii. confirm its reasonableness (i.e. it is consistent with, and does not otherwise conflict with the documentation collected in the course of opening the account (including AML/KYC information).</td></tr>
</table>

Type of Financial Accounts		Summary of the due diligence
Entity Accounts (i.e. accounts held by legal persons or arrangements). *Sections V and VI.*	**Preexisting Accounts** (i.e. as defined by domestic legislation – typically accounts opened prior the date of effect of the legislation implementing the CRS). *Section V.*	Option to exclude Preexisting Entity Accounts with a balance or value less than USD 250 000 from review (see Subsection 6.3.11 of the toolkit). *Section V(A).* For Preexisting Entity Accounts with a balance or value above USD 250 000, the Reporting Financial Institution must determine: **a)** whether the Entity itself is a reportable person **b)** whether the Entity is a Passive NFE and, if so, whether such Passive NFE has one or more Controlling Persons that are Reportable Persons. For purposes of determining the status of the Entity (i.e. if the Entity itself is a Reportable Person and if it is a Passive NFE), the Reporting Financial Institutions may (i) rely on information in possession of the financial institution (such as the AML/KYC file) and publicly available information (such as public records) or (ii) obtain a self-certification from the Entity. If applicable, for purposes of identifying the Controlling Persons of a Passive NFE, the Reporting Financial Institution may rely on AML/KYC documentation or obtain a self-certification. For purposes of determining if the Controlling Persons of the Passive NFE are Reportable Persons, the Reporting Financial Institution may rely on AML/KYC documentation, but only if the account balance or value does not exceed USD 1 million. If the balance or value exceeds this threshold, the Reporting Financial Institution must collect a valid self-certification.
	New Accounts (i.e. as defined by domestic legislation – typically accounts opened on or after the date of effect of the legislation implementing the CRS). *Section VI.*	Regardless of the balance or value of the account, all New Entity Accounts must be reviewed. For such purposes, a Reporting Financial Institution should: **a)** collect a valid self-certification, in order to determine **i.** whether the Entity itself is a reportable person and **ii.** (1) whether the Entity is a Passive NFE and, if so, (2) whether such Passive NFE has one or more Controlling Persons that are Reportable Persons, and **b)** confirm its reasonableness. A Reporting Financial Institution may not need to obtain a self-certification to the extent that it can reasonably determine, based on information in possession of the Financial Institution (such as the AML/KYC file) or publicly available information (such as public records), that the Entity is exempt from being reported. A Reporting Financial Institution may also determine that an entity is not a Passive NFE based on information in its possession or publicly available information.

FIGURE 5. **Reportable Accounts**



2.3.4. Effective implementation

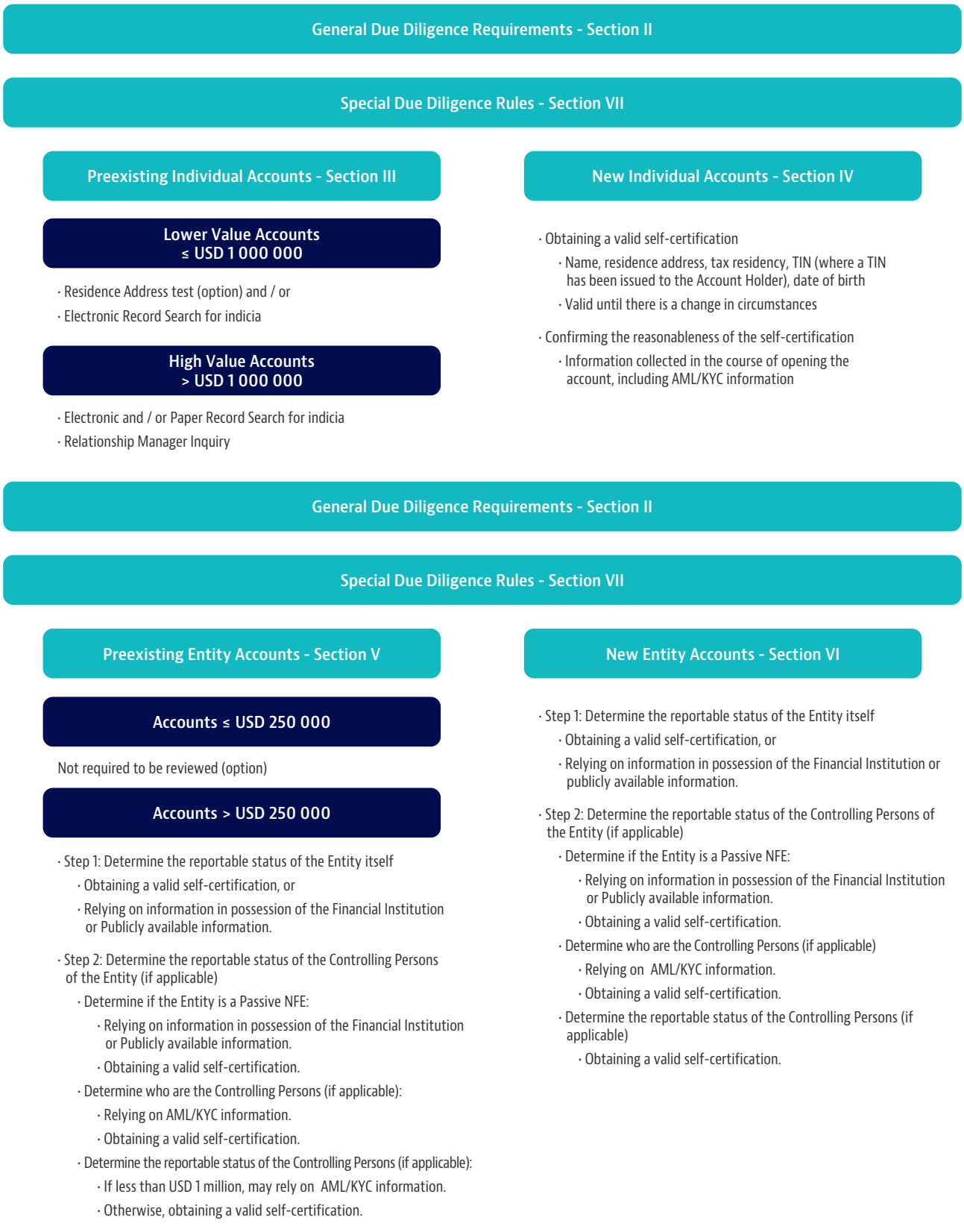
Section IX of the CRS relates to the rules and administrative procedures that a jurisdiction should have in place in order to ensure the effective implementation of, and compliance with, the CRS, including:

- domestic rules to prevent circumvention the CRS due diligence and reporting procedures (see Subsection 6.2.6 of the toolkit)
- requiring Financial institutions to keep records of its due diligence and reporting procedures for a sufficient period (see Subsection 6.2.3 of the toolkit)
- following up on undocumented accounts (see Section 7.1 of the toolkit)
- periodically reviewing jurisdiction-specific Non-Reporting Financial Institutions and Excluded Accounts (see Section 7.1 of the toolkit)
- having in place effective enforcement provisions to address non-compliance (see Section 7.1 of the toolkit).

2.4. THE MONITORING AND PEER REVIEW PROCESSES OF THE IMPLEMENTATION OF THE STANDARD ON AUTOMATIC EXCHANGE OF FINANCIAL ACCOUNT INFORMATION

The CRS-AEOI standard was a new standard when it was agreed in 2014. To support satisfactory implementation of the Standard by the 100 jurisdictions which committed to start exchanging in 2017 or 2018, a staged approach was established by the Global Forum to monitor, assist and assess CRS-AEOI implementation even during the implementation phase of the Standard. This was in recognition that certain issues could be

FIGURE 6. **High-level architecture of the CRS due diligence**



identified and addressed early in the implementation process, before the requirements of the Standard could be fully reviewed, as this would need exchanges to be taking place on a routine basis. This process has now led to the review of the effectiveness in practice of the implementation of the Standard.

In accordance with the staged approach, all committed jurisdictions have been subject to peer review processes to assess their compliance with the Standard.

Any newly committed jurisdictions will undergo the Global Forum's monitoring and peer review processes as part of their CRS-AEOI implementation journey.

2.4.1. The monitoring process

The 2017-18 committed jurisdictions were subject to a structured monitoring process, i.e. the staged approach, in advance of the first exchanges.

The staged approach commenced with a focus on monitoring key elements of the implementation of the CRS-AEOI standard to identify as soon as possible any areas where technical assistance may be required. The monitoring stage was critical to ensure the delivery of the commitments.

Subsequently, the Global Forum focused on areas that could usefully be reviewed in advance of exchanges taking place.

As a first step, the confidentiality and data safeguards framework of committed jurisdictions were reviewed under a pre-exchange review process aimed at ensuring that they meet good practice standards before the first exchanges could take place (see Subsection 2.4.2 of the toolkit).

This was followed by the legislative assessments of the domestic legal frameworks implementing the Standard, including assessments of jurisdiction-specific Non-Reporting Financial Institutions and Excluded Accounts low-risk lists (see Subsections 6.3.1 and 6.3.2 of the toolkit), to ensure that reporting and due diligence obligations are introduced in line with the Standard. Thereafter, the Global Forum monitored committed jurisdictions to ensure they had put in place CRS-AEOI exchange agreements with all Interested Appropriate Partners, including through the provision of a review mechanism that can be triggered if a jurisdiction is concerned about delays in putting in place any agreements. Finally, there was monitoring to ensure that jurisdictions had put in place the technical requirements to undertake exchanges.

All jurisdictions committed to start exchanging after 2018 are also subject to the monitoring process.

2.4.2. The peer review process

Jurisdictions committed to implement the Standard are subject to a peer review process which covers three main elements:

- the confidentiality and data safeguards framework
- the legal frameworks implementing the Standard
- the effective implementation of the Standard in practice.

All of these elements are reviewed against the CRS-AEOI Terms of Reference (ToR).

The ToR[33] were agreed by the Global Forum in 2018 and provide the basis against which the implementation of the Standard by jurisdictions is peer reviewed. They reflect the requirements necessary to effectively implement the Standard and incorporate legal and practical aspects.

The ToR are organised into three categories of Core Requirements (CRs), each of them composed of Sub-Requirements (SRs). Table 3 provides an overview of the ToR.

The assessment of the confidentiality and data safeguards framework follows a specific methodology and schedule.

The assessment of the legal framework and its effective implementation in practice is being conducted simultaneously for all jurisdictions committed to 2017-18 exchanges. In 2020, the Global Forum released the conclusions of the first peer reviews of the legal framework put in place by each of these committed jurisdictions and began the process of peer reviewing the effective implementation of the Standard in

33. The ToR are available at www.oecd.org/tax/transparency/documents/AEOI-terms-of-reference.pdf.

Table 3. **Extract from the Terms of Reference**

CR 1: Jurisdictions should ensure that all Reporting Financial Institutions apply due diligence procedures which are in accordance with the CRS to review the Financial Accounts they maintain, and collect and report the information required by the CRS.	**CR 1 Legal framework:** Jurisdictions should have a domestic legislative framework in place that requires all Reporting Financial Institutions to conduct the due diligence and reporting procedures in the CRS, and that provides for the effective implementation of the CRS as set out therein.
	CR 1 Legal framework: Jurisdictions should have a domestic legislative framework in place that requires all Reporting Financial Institutions to conduct the due diligence and reporting procedures in the CRS, and that provides for the effective implementation of the CRS as set out therein.
CR 2: Jurisdictions should exchange information with all interested appropriate partners in accordance with the CRS-AEOI standard, in a timely manner, ensuring it is collected, sorted, prepared, validated and transmitted in accordance with the CRS-AEOI standard.	**CR 2 Legal framework:** Jurisdictions should have exchange relationships in effect with all interested appropriate partners as committed to and that provide for the exchange of information in accordance with the Model CAA.
	CR 2 Effectiveness in practice: Jurisdictions should exchange the information effectively in practice, in a timely manner, including by collecting, sorting, preparing, validating and transmitting the information in accordance with the CRS-AEOI standard.
CR 3: Jurisdictions should keep the information exchanged confidential and properly safeguarded, and use it in accordance with the exchange agreement under which it was exchanged.	**CR 3.1:** Jurisdictions should have a legal framework that ensures the confidentiality and appropriate use of information exchanged under an international exchange agreement.
	CR 3.2: Jurisdictions should have an Information Security Management framework that adheres to internationally recognised standards or best practices and ensures the protection of exchanged information.
	CR 3.3: Jurisdictions should have enforcement provisions and processes to address confidentiality breaches.

practice,[34] the outcome of which will be published in 2022. The conclusions made on the legal framework are updated as necessary (e.g. if jurisdictions have made changes to their legal frameworks to address recommendations made) and published annually.

Jurisdictions committed to start their exchanges after 2018 are also subject to these review processes and follow an equivalent schedule.

Assessment of the confidentiality and data safeguards framework

The purpose of the Global Forum's peer reviews on confidentiality and data safeguards is to provide assurance that jurisdictions are meeting the legal and operational requirements, including information security management (ISM), to ensure that the data exchanged remains confidential and is adequately safeguarded.

These elements are reviewed against the requirements set out under CR 3.[35]

The assessments are conducted by experienced ISM officials drawn from peers' tax administrations acting in their individual capacity as ISM experts, with co-ordination by the Global Forum Secretariat.

The confidentiality assessments include:

- A pre-exchange assessment before data is exchanged for the first time. Pre-exchange assessments started in 2015 in the context of the staged approach.

34. The results of the reviews can be found in the *Peer Review of the Automatic Exchange of Financial Account Information 2021* available at https://doi.org/10.1787/90bac5f5-en.

35. The CR 3 is detailed in the ToR for the confidentiality and data safeguards assessments available at www.oecd.org/tax/transparency/documents/confidentiality-data-safeguards-assessments-tor.pdf.

- A post-exchange assessment that gauges the confidentiality and data safeguarding arrangements for CRS data after it is being exchanged. Post-exchange assessments commenced in 2019.

- A dedicated assessment process with respect to non-reciprocal jurisdictions, reflecting the fact that they send but do not receive CRS data.

The assessment process includes the completion of a questionnaire, an on-site visit, follow-up questions and peer comments. The report drafted by the assessment team is discussed and approved by the relevant peer review group, the AEOI Peer Review Group + (APRG+), then adopted by the CRS-AEOI peers and shared for information with all Global Forum members.

In general, the assessment process can take around six to nine months. Jurisdictions exchanging information for the first time, in particular, will need to consider these timelines to ensure that their pre-exchange confidentiality assessment is completed well before the time of the first exchanges, noting that time will also be needed for jurisdictions to update their lists of reportable jurisdictions (i.e. their lists of jurisdictions with respect to which information should be reported) and activate the associated exchange relationships.

Where serious confidentiality and data safeguarding weaknesses are identified, "hard" recommendations are issued and the jurisdiction's exchange partners will not be expected to send the jurisdiction information until improvements are made and a satisfactory re-assessment is concluded. In order to deliver on its commitment to implement the Standard, the jurisdiction would still be expected to exchange information on a non-reciprocal basis, unless the serious weaknesses also impact the collection and sending of the information. If required, the Global Forum Secretariat provides technical assistance to help implement the necessary improvements. "Soft" recommendations can also be issued where areas of improvement are identified.

Assessment of the legal framework

The Global Forum conducts peer reviews of the legal framework put in place to implement the Standard. These reviews cover:

- the domestic legislative framework that requires Financial Institutions to conduct the due diligence and reporting rules (ToR, CR 1)

- the international legal framework that allows for the exchange of CRS data (ToR, CR 2).

The result of the peer review of the legal framework is the assignment of a determination for each CR as well as an overall determination.[36] Jurisdiction reports are prepared by an assessment panel of experts drawn from CRS-AEOI peers and co-ordinated by the Global Forum Secretariat. The draft reports are then submitted for comments from CRS-AEOI peers (defined as those committed to start exchanging information under the Standard in a particular year and that have a domestic legislative framework in place). Subsequently, the final reports are approved by the relevant peer review group, the AEOI Peer Review Group (APRG) and adopted by CRS-AEOI peers and shared for information with all Global Forum members.[37]

Assessment of the domestic legal framework

The translation of the due diligence and reporting obligations set out in the CRS into the domestic legal framework of a committed jurisdiction and the introduction of relevant enforcement provisions are critical for the implementation of the Standard. Therefore, this element is subject to peer review.

CR 1 refers to the detailed due diligence and reporting procedures that Financial Institutions must follow. These are standardised procedures to ensure that Financial Institutions report the correct information on Financial Accounts and their Account Holders or Controlling Persons to the tax authority in a uniform manner. Table 4 sets out the elements reviewed.

To conduct the peer review process, committed jurisdictions are requested to:

- Provide the domestic legislative framework implementing the Standard. It includes the primary and secondary legislation, any related guidance developed that incorporate any of the requirements of the Standard as well as any relevant provisions of

36. Three possible determinations can be issued: (i) "In place", where no or very minor gaps have been identified; (ii) "In Place but Needs Improvement", where one or more deficiencies material to the proper functioning of elements of the standard have been identified; (iii) "Not In Place", where the gaps identified are viewed as creating a material risk to the overall operation of the standard.

37. The results of the reviews can be found in the *Peer Review of the Automatic Exchange of Financial Account Information 2021* available at https://doi.org/10.1787/90bac5f5-en.

Table 4. **Elements of the domestic legal framework reviewed under Core Requirement 1**

Assessment of CR 1 – Domestic legal framework	
Due diligence and reporting rules and enforcement framework	Review of: ● implementation of the scope of Reporting Financial Institutions ● scope of the Financial Accounts they must review ● detailed due diligence procedures that Financial Institutions must use to identify the Reportable Accounts ● information that must be reported ● legal framework to enforce the requirements.
Non-Reporting Financial Institutions and Excluded Accounts	Review to ensure that the jurisdiction-specific Non-Reporting Financial Institutions and Excluded Accounts provided for by each jurisdiction meet the requirements of the categories of the Standard or have substantially similar characteristics to those categories and pose low-risk of being used for tax evasion.
Any other legal frameworks relied upon to implement the Standard	Review of a jurisdiction's: ● definition of "beneficial owner" contained in its legislative framework implementing the FATF Recommendations, where relied upon for the identification of Controlling Persons ● pre-existing penalty and enforcement framework where it is relied upon to ensure compliance with the Standard.

the jurisdiction's pre-existing legal framework. The domestic legislative framework should be provided in English or French.

- Complete a checklist aimed at demonstrating how each of the requirements of the Standard have been introduced into the domestic legislative framework. The checklist process reviews the core elements of the legal implementation of the Standard, including all of the requirements contained in the CRS and all of the key requirements contained in its Commentary.
- Submit templates on the jurisdiction-specific Excluded Accounts and/or Non-Reporting Financial Institutions where such exclusions have been provided for. The template review process is to confirm that these exclusions meet the requirements set out in the Standard.

Where the review identifies gaps in a jurisdiction's domestic legislative framework, a "recommendation" is made to the assessed jurisdiction to address the deficiency. In some cases, where there is lack of clarity in any aspect of the legal framework and its application in practice, a "note" is made to the assessed jurisdictions to monitor the issue identified to ensure it operated effectively in practice.

Assessment of the international legal framework

The establishment of an international legal framework that allows for automatic exchange with all interested appropriate partners is also a key requirement of the CRS-AEOI ToR.

Under CR 2, the Global Forum reviews whether:

- The assessed jurisdictions have put in place exchange agreements with all Interested Appropriate Partners. If a partner raises concerns with respect to the delay of an assessed jurisdiction in putting in place an exchange agreement, a peer review process may be triggered whereby the causes of such delay are analysed and any necessary recommendations can be made.
- The agreements are in line with the Model CAA. Where an exchange agreement other than the CRS MCAA (which is already modelled on the Model CAA) is put in place with a particular partner (e.g. a bilateral CAA), its provisions are reviewed. To that end, the assessed jurisdiction is required to provide the corresponding agreement in English or French and complete a checklist through which the required elements of the agreement are assessed.

Table 5 summarises the elements reviewed.

Overview of the implementation of the standard and its monitoring and assessment framework

Table 5. **Elements of the international legal framework reviewed under Core Requirement 2**

Assessment of CR 2 – International legal framework	
Identification of the interested appropriate partners. A peer review process may be triggered.	A process to facilitate jurisdictions identifying their interested appropriate partners. A jurisdiction may trigger a peer review mechanism if it becomes concerned with respect to delays in a particular potential partner putting in place an exchange agreement with them.
Review of exchange agreements contents.	Where a jurisdiction puts in place an exchange agreement to exchange information with a particular partner other than the CRS MCAA, a review of the provisions of such exchange agreement is carried out to ensure they are in accordance with the requirements of the Standard.

Assessment of the effectiveness in practice

Under the ToR, a jurisdiction must also ensure that the Standard operates effectively in practice. This includes ensuring that Financial Institutions collect and report the information required, including by having an effective administrative framework to ensure the effective implementation of the Standard by Financial Institutions (CR 1) and exchanging the information effectively in practice (CR 2). Table 6 sets out the elements reviewed.

Table 6. **Elements of effectiveness in practice reviewed under Core Requirements 1 and 2**

Assessment of CR 1 – Effectiveness in practice	
Ensuring that Financial Institutions collect and report the information required, including by having an effective administrative framework to ensure compliance.	A compliance strategy implemented, that is based on a risk assessment which takes into account a range of relevant information sources. Procedures to ensure that Reporting Financial Institutions are reporting information as required. Verification procedures to ensure that the information being reported is complete and accurate, including assessing the records maintained by Reporting Financial Institutions.
International collaboration to ensure effectiveness.	Procedures to collaborate on compliance and enforcement with exchange partners, in particular by effectively following up on notifications of errors or possible non-compliance received from exchange partners.
Assessment of CR 2 – Effectiveness in practice	
Preparing and validating the information.	Procedures to sort, prepare and validate the information reported by Reporting Financial Institutions in accordance with the technical requirements, to ensure that the information is ready to be sent.
Using secure channels to exchange the information.	Ensuring that the information is kept safe while it is being transmitted. This is normally ensured by using the CTS.
Receipt of information.	Systems in place to receive information and to send a status message to the sending jurisdictions in accordance with the CRS Status Message XML Schema and the related User Guide.
Timeliness in the exchanges and follow-up.	The timeliness of the exchanges, including the timeliness of any response to follow-up from a jurisdiction's partners and the provision of additional or amended information as necessary.

Table 7. **Assessment timeline for post-2018 committed jurisdictions**

Example of a jurisdiction committed to start exchanging under the Standard in September of year Y.

Before September Y	September Y	Y+2	Y+4	After September Y
Pre-exchange assessment of the confidentiality and data safeguards framework	**First exchange**	**Assessment of the legal frameworks implementing the Standard**	**Assessment of the effective implementation in practice**	**Post-exchange assessment of the confidentiality and data safeguards framework**
• Identification of any gaps prior to the exchanges • Identification of jurisdictions in need of assistance to comply with the confidentiality and data safeguards standards The assessment can lead to hard recommendations or soft recommendations depending on the seriousness of the gaps identified. Where serious deficiencies are identified, then they should be addressed before exchanges commence.	Exchanges can take place on a reciprocal or non-reciprocal basis.	• Domestic legislative framework ensuring collection and reporting of the information • International legal framework ensuring the exchange of information The assessment of these two elements is done via checklists and result in the issuance of recommendations and/or notes. Determinations are provided for CR 1 and 2 as well as an overall determination.	• Ensuring that legal frameworks are implemented and operate effectively in practice and that Financial Institutions collect and report the required information • Implementation and usage of compliance procedures etc. The assessment of these elements is done via a questionnaire and other sources and result in the issuance of recommendations. Ratings are provided for CR 1 and 2 as well as an overall rating.	• Identification of any gaps or areas of improvement The assessment can lead to hard recommendations or soft recommendations with respect to CR 3 depending on the seriousness of the gaps identified. Where serious deficiencies are identified, the jurisdictions will need to address them to exchange.
This assessment needs to be finalised before a jurisdiction commences exchanging information under the Standard. It is recommended to start the review as soon as the jurisdiction is ready and to finalise it well in advance of the first exchanges to maximise the number of sending partners for the first exchanges. Generally, the review should start not later than the middle of the year preceding the year of first exchanges (Y-1).		The assessments can start as soon as the relevant legal framework is in place. This would allow time for the jurisdiction to address any recommendations before the results are published. The results of assessment of the legal framework is are compiled into a report, along with a determination, and published in the second year after the first exchanges have taken place.	This assessment starts three years after the assessed jurisdiction commenced exchanges under the Standard and lasts for two years.	This assessment takes place after exchanges have commenced and is subject to a specific assessment schedule.

Overview of the implementation of the standard and its monitoring and assessment framework

There are three sources of information used to assess a jurisdiction's effective implementation in practice:

- The peer input questionnaire, where exchange partners of the assessed jurisdiction provide input on the timeliness and quality of the information received.
- The assessed jurisdiction is also requested to provide details of its administrative framework to ensure Financial Institutions comply with the CRS due diligence and reporting procedures through the administrative compliance framework questionnaire. This questionnaire requests information relating to all requirements under the ToR, including details on the activities conducted and results achieved.
- Information from other sources, including external sources of information, can also be considered as part of the assessment.

The peer review process is similar to the process conducted for the assessment of the legal framework. A rating will be allocated to each CR and an overall rating will be attributed to each committed jurisdiction. The outcome of the effectiveness reviews of the 2017-18 committed jurisdictions should be published in 2022.

Where the review identifies gaps in the administrative framework implementing the Standard, a "recommendation" is made to the assessed jurisdiction to address the deficiency.

The timeline of the assessments of post-2018 committed jurisdictions

The timeline of the assessments depends on each jurisdiction's date of commitment to start exchanging under the Standard. Table 7 outlines the timeline of assessments for jurisdictions committed to commence exchanges under the Standard after 2018.

3. Implementation strategy

The implementation of the Standard in a jurisdiction should be conceived as a multi-work stream, medium-term project, the realisation of which should be based on a clear strategy. This strategy is the process by which the jurisdiction will translate its commitment to implement the Standard by a certain date into an action plan and related activities to achieve the defined objective: exchanging CRS data as scheduled and ensuring that the information being exchanged is complete and accurate. The action plan defined at senior level will steer the work of the diverse stakeholders in the direction set out in the strategy.

The implementation strategy starts with the decision to commit to start CRS-AEOI exchanges by a specific date.

Once a jurisdiction is committed it should (i) develop a comprehensive action plan with clear activities, timelines and responsible persons, (ii) follow up the implementation of the actions and activities, (iii) take corrective measures if needed, and (iv) regularly report on the status of the implementation.

To ensure that the jurisdiction takes an informed decision and meets its objective, the Global Forum Secretariat provides support and guidance in the pre-commitment phase and accompanies the jurisdiction in the commitment process, its delivery and the use of the exchanged data.

3.1. COMMITTING TO IMPLEMENT THE STANDARD BY A SPECIFIC DATE

All Global Forum members are committed to implement the CRS-AEOI standard. However, developing countries that do not host a financial centre are not required to implement the Standard by a specific date. In recognition of the challenges they may face, these developing countries are committed to implement the Standard to a practical timeframe. To this end, they receive technical assistance from the Global Forum Secretariat and other development partners.

The successful implementation of the Standard requires a jurisdiction to take an informed decision on its commitment date. The date chosen for the first CRS-AEOI exchange should be realistic and based on an assessment of what implementation requires and the resources that will need to be dedicated to it.

Based on its experience in assisting jurisdictions to implement the Standard since 2015, the Global Forum Secretariat has renewed and strengthened its strategy for supporting developing countries in benefiting from the Standard.[38] Lessons learned from the assistance provided under its 2017 *Plan of Action for Developing Countries' Participation in AEOI*[39] have also informed the Global Forum Secretariat's strategy.

3.1.1. Defining a realistic date for the first exchanges under the Standard

Jurisdictions that are considering the implementation of the Standard in the medium-term are encouraged to engage with the Global Forum Secretariat to inform their decision before formally committing to start their first exchanges under the Standard by a specific date.

Pre-commitment support is available to provide the jurisdiction with relevant information, guidance and advice to define what could be a realistic date for the first exchanges, taking into account the specific circumstances.

The support available covers the following main elements:

- raising awareness on the requirements of the Standard, the benefits of implementing it, and the commitment process, including its implications
- unpacking the Standard to explain the building blocks for its effective implementation
- conducting a preliminary assessment of the ISM maturity level in place in the tax authority
- defining an action plan for the implementation of the Standard
- answering any questions the jurisdiction may have.

The preliminary assessment of the ISM maturity level is a critical element to helping a jurisdiction determine a commitment date. A jurisdiction's ability to receive CRS data from its partners is dependent on a positive review by the Global Forum of the confidentiality and data safeguards framework in place in the jurisdiction. Therefore, a jurisdiction should assess whether its current framework adheres to internationally recognised standards or best practices in this area. If gaps are identified, then the jurisdiction should consider the time needed to address them. By conducting a preliminary assessment and formalising it in a technical assistance report, the Global Forum Secretariat will assist the jurisdiction in identifying the potential gaps, defining an action plan to address them and deciding on the appropriate date for the first exchanges.

It is also important to consider the time needed to draft the necessary legal provisions and to bring them into effect. The timeline to do this will determine the time from which Financial Institutions will begin collecting the information to report, noting that this will require them to implement the necessary systems changes. Once the information is being collected, it will be reported to the tax authority and exchanged during the following year.

3.1.2. The commitment process

To commit to implement the Standard and start CRS-AEOI exchanges by a certain date, a letter containing the required commitments should be signed by the minister of finance (or any other persons authorised to engage the jurisdiction) and sent to the Chair of the Global Forum.

The commitment entails:

- Reciprocity in both sending and receiving information (although jurisdictions may elect to only send information, which may be appropriate for jurisdictions that do not have an income tax).
- Exchanging with all interested appropriate partners, being all those jurisdictions that are interested in receiving information from the jurisdiction and that meet the expected standards in relation to confidentiality, data safeguards and proper use of the information.
- Commencing information exchanges within a specific date, which is referred to in the letter.

A template letter containing all the required commitments is available to the interested jurisdiction upon request to gftaxcooperation@oecd.org.

38. Global Forum Secretariat / OECD (2021), *Unleashing the potential of automatic exchange of information for developing countries – 2021 Strategy*, available at www.oecd.org/tax/transparency/documents/aeoi-strategy-developing-countries.pdf.

39. Global Forum Secretariat / OECD (2017), *The Global Forum's Plan of Action for Developing Countries Participation in AEOI*, op. cit.

Acknowledging that unforeseen circumstances may affect the delivery of the commitment made, a developing country which does not host a financial centre may request a postponement of its commitment by letter to the Chair of the Global Forum describing these circumstances and indicating a reasonable new date for the full implementation of the Standard.

A committed jurisdiction is subject to the Global Forum's monitoring and peer review processes (see Section 2.4 of the toolkit). The commitment will be reflected in the Automatic Exchange Portal (see Subsection 2.1.5 of the toolkit) and the status of the implementation of the Standard will be regularly provided to the Global Forum and the G20. Capacity building can be provided upon request to the committed jurisdiction at each stage of the implementation of the Standard as well as on the use of CRS data.

3.2. DEVELOPING AND IMPLEMENTING THE STRATEGY

3.2.1. Setting up an organisational framework

The role of the implementation committee

The translation of the political decision into concrete actions and activities should be assigned to an implementation committee as the implementation of the Standard usually requires a strong communication and coordination between different stakeholders within and outside of the tax authority.

- Within the tax authority, the implementation of the Standard will require the contribution of several functions such as the legal, audit, taxpayer management, IT, security and procurement functions.
- Other public authorities should also be engaged in the implementation of the Standard such as the ministry of finance, the financial sector supervisors, the ministry of justice, the ministry of foreign affairs, the body responsible for supervising the passage of all legislation through Parliament and the data protection authority.
- Other stakeholders should also be consulted in the relevant implementation phases, such as the financial sector (e.g. through the Financial Institutions associations (bankers' association, insurance association, investment entity association) and customer associations.

Depending on the size of the jurisdiction, different approaches can be followed:

- A small jurisdiction may establish a single committee that can meet in restricted or enlarged format depending on the matter to be discussed and authorise, when relevant, the participation of business and customer associations.
- A large jurisdiction may choose to have a high-level committee that makes strategic decisions and directs the work of a more technical committee that is responsible for the implementation of actions and activities, including consultation with business and customer associations.

A jurisdiction should determine what organisation would best fit its own circumstances in order to achieve the objective assigned at political level. To that end and irrespective of the approach taken, senior officials should be involved in the implementation committee which should be chaired by a person that has sufficient authority (e.g. the head or deputy head of the tax authority, the secretary general of the ministry of finance). Since members with sufficient seniority to drive forward the necessary changes are likely to be too busy to attend all the meetings of the committee, ideally a deputy should also be assigned.

The committee should meet on a regular basis using different formats when relevant (e.g. thematic meetings every two weeks, general meetings every month). The plenary committee should at least meet every two months with the participation of senior officials.

The implementation committee should therefore have a clear mandate from the minister of finance (or the government) to carry out its activities. The mission of the committee is to develop an action plan, plan the activities to be performed, monitor their completion and implement any necessary corrective measures to meet the objective, i.e. starting the first CRS-AEOI exchanges as scheduled. The committee should regularly report on the status of the implementation of the Standard to the minister of finance or the government and propose possible decisions and actions where needed.

Composition of the implementation committee

The identification of the relevant stakeholders to include in the committee is critical. To that end, the jurisdiction

should refer to the content of the implementation building blocks.

- The setup of the international framework (e.g. the MAAC and the CRS MCAA) is likely to require the involvement of the ministry of foreign affairs and communication with the Parliament.

- The adoption of the necessary legal framework will certainly require the coordination between the legal function of the tax authority with the relevant other authorities involved in the legislative procedure (e.g. ministry of justice, attorney general office, Parliament) as well as the financial sector supervisors. This is critical to ensure that the strict drafting parameters are followed and that the legislative process proceeds smoothly. To support the legislative process and facilitate compliance, communication actions should also be implemented which may include consultation with the relevant bodies.

- Meeting the confidentiality and data safeguards requirements would require the coordination between different functions of the tax authority or the ministry of finance (e.g. competent authority, internal audit, human resources, IT, security, legal, and procurement) but also with other authorities such as the data protection and the national cybersecurity authorities, and the external audit body.

- To proceed to the exchanges, ensure compliance with the CRS and effectively use CRS data, administrative and IT resources should be allocated. It may involve for instance the procurement of IT tools or systems, putting in place a method of transmission such as by linking to the CTS, the recruitment of officers (e.g. tax auditors, data scientists, information security officers or security experts), the training of staff, and the review of procedures and processes. Therefore, the relevant functions within the tax authority or the ministry of finance will need to be involved in the implementation of the Standard. In addition, other authorities may be involved such as the ministry of budget or the ministry of civil service. Engagement with financial sector supervisors is also critical in the design and implementation of the administrative compliance framework.

3.2.2. Strategic decisions

The implementation committee should make the relevant strategic decisions or refer to the relevant authority so that the decisions are taken in a timely manner.

Some key decisions need to be taken at the early stage of the implementation. This section will briefly introduce them while they will be further described in the following parts of the toolkit.

In general, jurisdictions have implemented the Standard within a period of 2-3 years. A few jurisdictions managed to implement it in a shorter timeframe while a few others needed a bit more time to complete it. In most of the cases, the 3-year timeline allows for a smooth completion of the implementation of all the requirements to effectively start the exchanges. Table 8 provides an example of an implementation within three years of the Standard. The planning of the different actions and activities is therefore crucial for the delivery of the commitment. Planning actions to implement in reverse order from the date of first exchange can be a useful exercise.

International legal framework

A key decision to take as early as possible is whether a bilateral or multilateral approach should be followed to setup a network of agreements allowing for CRS-AEOI with all interested appropriate partners. While this issue is further discussed in Part 5 of the toolkit, the recommended approach, and the approach followed by all other implementing jurisdictions, is to follow the multilateral approach through the combination of the MAAC and CRS MCAA. To do otherwise would require all other jurisdictions to be content with putting in place a series of bilateral agreements rather than continuing the multilateral approach they have put in place.

Irrespective of the approach chosen, the jurisdiction should determine whether the obligations derived from the international agreement would require (i) domestic legislative changes (e.g. lifting bank secrecy for EOI for tax purposes) and (ii) specific domestic procedures to be fulfilled (e.g. parliamentary or cabinet approval for signing the agreement, and/or ratification or approval of the agreement by the Parliament). In particular, while a CAA for CRS-AEOI is generally considered as an administrative agreement, some jurisdictions may need to follow some specific domestic procedures to be able to sign it and bring it into effect.

Table 8. **Example of a 3-year implementation timeline of the core CRS-AEOI components**

CRS-AEOI components	First year of implementation (Year-2 of the first exchange)	Second year of implementation (Year-1 of the first exchange)	Third year of implementation (Year of the first exchange)
International legal framework	MAAC signed and ratified, and ratification instrument deposited by end of August.		
	CRS-MCAA signed	CRS-MCAA activated.	
Domestic legal framework	Consultation with Financial Institutions.	Domestic legal framework in force	
	Adoption of the primary and secondary legislation (preferably at least six months before its entry into force or in effect).		
	Adoption and launch of a VDP programme.	VDP continues.	VDP is closed.
Due diligence		Due diligence starts	First reporting by Financial Institutions (preferably in May, June or July).
AEOI portal	Development and testing.		Production status (preferably in May, June or July).
Confidentiality and data safeguards	Global Forum's pre-exchange assessment undertaken (at the latest in June Y-1) and finalised, preceded by support and technical assistance from the Secretariat on confidentiality and data safeguards as necessary.		
CTS	Enrolment, test.		Production status before September.
CRS-AEOI exchange			September – first CRS-AEOI exchange.
Compliance	Compliance activities: from preventive and educational actions to verification and enforcement measures.		

The international legal framework should be in force and have taken effect in due time. For instance, a jurisdiction committed to start its first exchanges in September Y and relying on the MAAC should ideally sign and ratify the MAAC, and deposit the instrument of ratification by end of August of the year following the first reportable calendar year under the Standard (i.e. Y-2). This would avoid the need to lodge a unilateral declaration that will give effect to the MAAC for administrative assistance related to taxable periods earlier than its entry into force, which also reduces the number of partner jurisdictions for that reportable period (see Section 5.3 of the toolkit). In addition, the CRS MCAA should be activated as soon as possible (i.e. by end of Y-1 at the latest) to ensure that

as many partners as possible have time to review their list of Reportable Jurisdictions; otherwise the jurisdiction may only receive data from a limited number of partners for the first reportable period.

Domestic legal framework

Legislative timeline

Policymakers, along with the legal drafters, will also need to begin work on drafting legislation in sufficient time to ensure that the jurisdiction remains on course to commence exchanges as planned.

The latest date by which the domestic laws must be in place and take effect should be the start the full calendar year before the first year of exchange – year Y – (i.e. 1 January Y-1). This is because Financial Institutions must carry out the due diligence specified in the CRS and its Commentary in order to identify which information is reportable. As the Financial Institutions should start their due diligence the first day of the first reportable calendar year (i.e. 1 January Y-1), for example with respect to Financial Accounts opened from that day onwards (New Accounts). It is therefore recommended that the legislation is adopted sufficiently in advance to give time to the Financial Institutions to comply with their CRS obligations (e.g. by June Y-2). It should also be recognised that for Financial Institutions to commence the collection of the information they will need to put in place the necessary systems and processes, which will also take some time. A jurisdiction wishing to begin exchanges in September 2024 should therefore have a legislative basis in place which takes effect and requires due diligence to be carried out from 1 January of 2023.

Jurisdictions should therefore start the legislative work as early as possible and work backwards from the first year in which Financial Institutions will be required to carry out due diligence (Y-1). Key factors to consider will be:

- **Legislative adoption timetable (or equivalent):** Commitment from governments to implement the Standard should mean that parliamentary time will be set aside for consideration and adoption of the necessary legislation. Policymakers will need to ensure that the legislative process is complete in sufficient time to allow the legislation to take effect before the start of Y-1. Primary legislation can often take substantial time to bring into effect. Should the jurisdiction decide to implement domestic legislation with both primary and secondary legislation and/or binding guidance, additional time may be needed to issue secondary legislation and/or guidance and ensure it can take effect from 1 January Y-1.
- **Drafting process:** Jurisdictions will need to factor in time to draft the necessary legislation. Where the jurisdiction chooses to implement legislation using the model rules developed by the Global Forum Secretariat (see Section 6.1 of the toolkit), consultation with government legal services or translation services may still be needed to adapt the model rules as required.
- **Consultation with stakeholders:** Jurisdictions may have a legislative requirement to hold consultations before the introduction of new policy or legislation, or they may wish do this as a mark of good practice (see Box 1).

Box 1. **Consultation with stakeholders**

The CRS and its Commentary are purposefully prescriptive to ensure a level playing field across all jurisdictions and to maximise consistency across the data exchanged. Any adaptations to draft legislation following consultation with stakeholders may therefore be more constrained than is typically the case in policymaking.

Nevertheless, jurisdictions may wish to work closely with their financial industry and their financial supervision authorities, when choosing whether to adopt certain optional approaches under the CRS, or when determining whether to introduce jurisdiction-specific Excluded Accounts or Non-Reporting Financial Institutions.

Consultation with industry also serves the helpful purpose of informing Financial Institutions from an early stage of their forthcoming obligations. As Financial Institutions will often need to implement IT tools to comply with the CRS due diligence and reporting requirements and amend on-boarding processes for customers, preparing industry for forthcoming legislation will contribute to a smoother implementation of the Standard by industry and should facilitate higher rates of compliance.

Other legislative considerations

The approach to follow for the translation of the CRS into the domestic legal framework should also be discussed in advance. Section 6.2 provides guidance on different possibilities ("copy out" and "reference" methods) for the legislative implementation of the CRS, which needs to be considered carefully. The interaction between the way domestic legislation is drafted and the requirements of the CRS is an area of attention as deviations from the text of the CRS may lead to legislative deficiencies and non-compliance.

Another element to include in the legislative decision is which authority or authorities will monitor and supervise compliance with the CRS obligations. This decision should be made as soon as possible to verify that the relevant enforcement powers and measures are in place or ensure their inclusion in the legal framework (see Section 6.2 and Section 7.1 of the toolkit).

Finally, the implementation of a VDP is also a strategic issue to discuss with all relevant authorities (see Part 4 of the toolkit) as it will need to be implemented in anticipation of the first exchanges and requires the adoption of the legislation as well the organisational framework and the related procedures.

Securing the necessary administrative and IT resources

CRS-AEOI exchanges are carried out in an electronic format and involve a large volume of data. Therefore, dedicated resources should be devoted to the implementation of the Standard to ensure that the activities are delivered as scheduled, officials are trained and systems are implemented in advance of the first exchanges.

The needs should be assessed as soon as the implementation project is established. Depending on the needs identified, gaps to be addressed or the approach decided (in-house, outsourcing), strategic decisions should be taken. They may include the following:

- recruitment of new staff with specific skills (e.g. data scientists, information security officers, IT specialists, tax auditors, financial industry experts) or redeployment of existing staff, and establishment and execution of a training programme in these specific areas
- training of staff on the relevant aspects of the CRS
- organisational changes related to the setup of an administrative framework to ensure compliance of Financial Institutions with their CRS obligations
- improving the confidentiality and data safeguards framework
- strengthening the IT infrastructure
- building or procuring an AEOI portal to receive information from Financial Institutions and to prepare the files to be shared with partner jurisdictions (see Section 7.2 of the toolkit)
- participation in the CTS, which requires signing the contract, paying the annual fee and connecting to the CTS (see Section 7.2 of the toolkit).

Administrative and IT resources will also be required beyond the implementation phase to:

- ensure the maintenance, the evolution and the security of the AEOI portal and the domestic systems implemented to use CRS data
- ensure a continued satisfactory level of confidentiality and data safeguards
- staff the unit in charge of handling CRS data (e.g. the EOI unit, a dedicated unit), communicating with exchange partners and liaising internally to solve any issues
- implement an administrative compliance framework and supervise compliance of Financial Institutions with their CRS obligations.

Ensuring an appropriate level of communication

The implementation of the CRS requires communication campaigns targeting different audiences as it progresses. While the communication issue can be dealt with on an *ad hoc* basis, there are circumstances where the communication should be discussed and coordinated at the implementation committee level. This is the case, for instance, when a VDP is considered.

Communication activities targeting Financial Institutions should be carried out as it will contribute

to compliance with the Standard. The content of the communication may vary depending on the different stages of implementation. For instance, awareness raising campaigns may be sufficient at the early stage, whereas training, consultation and guidance may be required at the later stage. In addition, the approach may vary depending on the specific circumstances of the jurisdiction. The communication can be done by the tax authority and/or the regulatory body, and it could focus on the business associations or could target all the Financial Institutions. A special hotline can be implemented as well as a dedicated website with all relevant information and documentation. Answering questions and solving doubts is critical to ease the implementation of the Standard and increase compliance.

Communication to the public at large is also an important consideration. It will support the understanding of the new on-boarding procedures when opening a new account, in particular the collect of a self-certification from the Account Holder or the Controlling Person by the Financial Institutions. It will also contribute to voluntary compliance by taxpayers, including through a VDP. If taxpayers are informed that their tax administration will soon receive data on any offshore financial assets they hold, this should prompt them to ensure that their affairs are in order, and to regularise their affairs where needed. To that end, different activities can be carried out such as social media campaign, interviews in newspaper, radio and/or television, and dedicated website with relevant information and documents. Specific actions should also be considered towards legal and accounting professionals who can advise their client on CRS issues.

3.3. THE SUPPORT PROVIDED BY THE GLOBAL FORUM SECRETARIAT

The Global Forum Secretariat is committed to support all jurisdictions at the different stages of their implementation journey.

The knowledge development tools[40] developed by the Secretariat are aimed at:

- raising awareness of officials on the requirements of the Standard
- assisting jurisdictions with the effective implementation of the Standard
- supporting jurisdictions in implementing a satisfactory confidentiality and data safeguards framework
- helping jurisdictions with their strategy to use CRS data
- guiding jurisdictions with their operational issues (AEOI portal, CTS).

Regional workshops and trainings are also regularly proposed to officials of the tax authority and any other authorities involved in the effective implementation of the Standard (e.g. regulatory authorities). Where relevant, in-country workshops are delivered.

Committed jurisdictions can benefit from comprehensive technical assistance activities to support the effective implementation of the Standard. This includes assistance in the following main areas:

- development of an implementation action plan
- participation to the consultation with the financial sector
- signing and ratification of the MAAC
- signing and activation of the CRS MCAA
- drafting of the domestic legislative framework to introduce the CRS
- definition and implementation of a VDP
- design of a compliance framework
- participation in the CTS
- consideration related to the AEOI portal (including issues related to security, validation and encryption)
- confidentiality and data safeguards, including ISM
- effective use of CRS data
- preparation of the peer review process.

Any questions or requests can be addressed to the Global Forum Secretariat (gftaxcooperation@oecd.org).

40. Available at www.oecd.org/tax/transparency/resources.

4. Voluntary disclosure programme

The establishment of a VDP may be relevant for a jurisdiction implementing the Standard. A VDP offers a number of benefits to the tax authority, including improving voluntary tax compliance. Such programmes have been very successful for the 2017-18 committed jurisdictions which have implemented them, with an impressive amount of revenue collected.

The following sections provide practical guidance on the design and implementation of a VDP in the context of the implementation of the Standard. Further policy recommendations and country examples can be found on VDPs more generally in the publication "*Update on Voluntary Disclosure Programmes – A Pathway to Tax Compliance*".[41]

4.1. WHAT IS A VOLUNTARY DISCLOSURE PROGRAMME?

VDPs are opportunities offered by tax authorities for taxpayers to correct their affairs under favourable conditions. VDPs offer a pathway for taxpayers to regularise their status, facilitating the collection of missing revenue for governments through limited administrative resources. As a cost-effective policy, VDPs deliver revenue while avoiding costly and contentious audits, litigation and criminal proceedings.

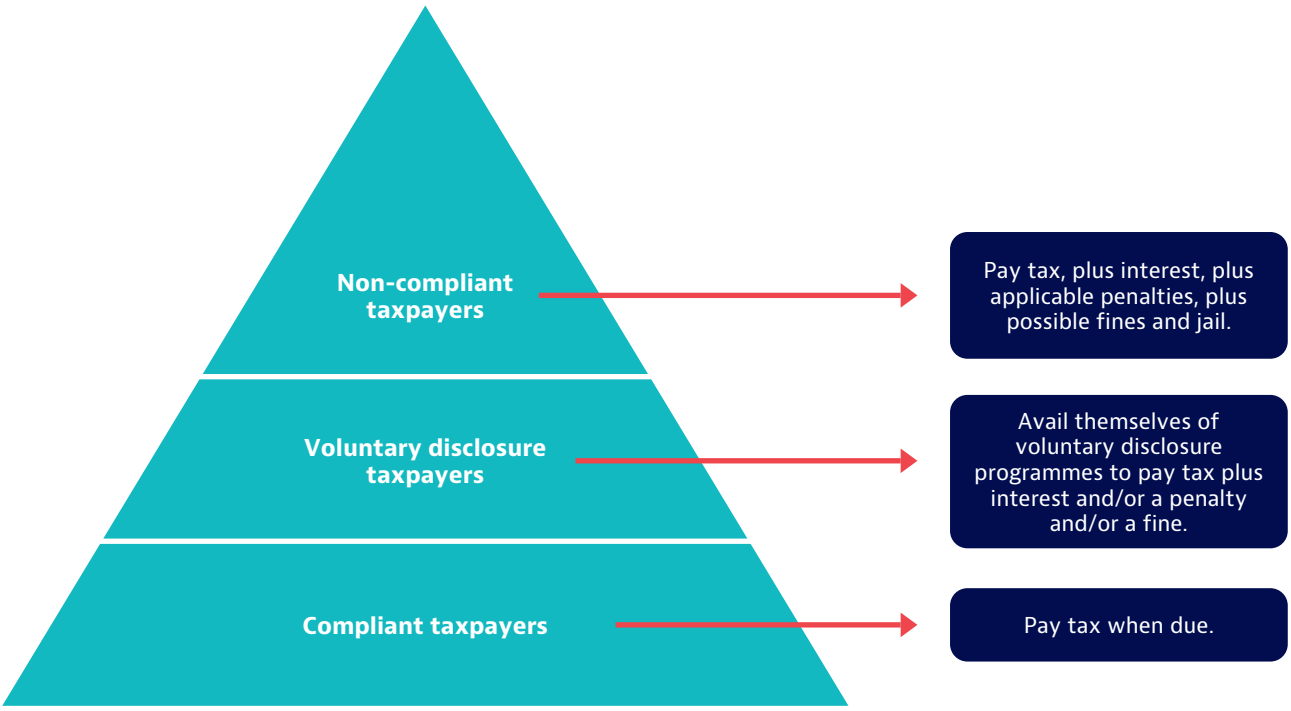
VDPs are presented to taxpayers as an opportunity to regularise non-disclosed assets and income under preferential terms and conditions. A VDP launched in the build-up to CRS-AEOI implementation is the last chance for taxpayers to disclose offshore interests before tax authorities start receiving information from partner jurisdictions. These programmes generally include incentives for taxpayers, such as reduced penalties and interest charges, together with some form of protection from prosecution.

As represented in Figure 7, the majority of taxpayers with offshore interests comply with the disclosure rules from their jurisdiction of residence. Non-compliant taxpayers can be divided into two categories:

- Taxpayers willing to correct their situation through VDPs due to the upcoming implementation of the Standard.
- Taxpayers that will continue to evade their tax obligations and search for strategies to hide assets offshore.

41. OECD (2015), *Update on Voluntary Disclosure Programmes – A Pathway to Tax Compliance*, available at www.oecd.org/ctp/exchange-of-tax-information/Voluntary-Disclosure-Programmes-2015.pdf.

FIGURE 7. **The compliance pyramid and voluntary disclosure**



Source: OECD (2015), *Update on Voluntary Disclosure Programmes, A pathway to Tax Compliance*.

As a result of international cooperation and access to CRS data by tax authorities, tax evaders face an increasing risk of detection and may be receptive to VDPs as an opportunity to amend their situation under more favourable conditions than those that would apply if they do not voluntarily disclose their foreign assets. The programme should therefore reach out to these taxpayers receptive to VDPs and bring them into voluntary compliance through a full regularisation of their tax affairs.

However, a number of taxpayers without interest in correcting their irregular situation will not be convinced by VDPs. As these taxpayers feel that their non-compliance will remain undetected, they will continue to take risks and avoid disclosure. To address this small part of the population, tax authorities should use CRS data for compliance actions (i.e. tax audits and investigations) and the full force of the law through penalties and criminal prosecution.

4.2. WHY CONSIDER A DISCLOSURE PROGRAMME AS PART OF THE IMPLEMENTATION STRATEGY OF THE STANDARD?

When a jurisdiction commits to implement the Standard, its ultimate goal is usually the reciprocal exchange of CRS data – which includes receiving information on financial accounts held by its residents in other jurisdictions. By expanding its EOI network and meeting the requirements to be considered an Interested Appropriate Partner, the jurisdiction positions itself to receive CRS data from a large number of partners.

When CRS-AEOI becomes fully operational, the tax authority will receive information from exchange partners on financial accounts held by its residents, including taxpayers that have not previously disclosed their offshore assets. As a result, taxpayers with undisclosed offshore interests face a soaring risk of detection once CRS data is exchanged.

The steady implementation of the Standard across jurisdictions over the past years has moved the goalposts in the offshore evasion space. For taxpayers with undisclosed offshore interests, the likelihood of detection increases.

In implementing jurisdictions, VDPs can be presented as the last chance for a taxpayer to become fully compliant before CRS data is received. While the risk of detection

is a clear incentive for non-compliant taxpayers to join a VDP, tax authorities also have much to gain with these programmes. In reaching out to reluctant taxpayers and offering a set of terms and conditions for the disclosure of offshore interests, a tax authority will benefit in the following ways:

- Avoid multiple administrative procedures and litigation cases against taxpayers, which have an uncertain outcome and can be very lengthy and costly.
- Quickly collect revenue, some of which could fund the implementation of the Standard, including specialised tax audit units, requirements on confidentiality and data safeguarding, IT infrastructure and systems.
- Ensure the reporting of these assets and the income generated by them (or the income transitioning through the Financial Accounts) in the subsequent years.
- Attract non-compliant taxpayers back into voluntary compliance, resulting in an expanded tax base, an increase in the legitimacy of the tax system and the promotion of further cooperation initiatives.
- Gather intelligence from taxpayers that join the VDP, increasing the knowledge of tax authorities in relation to offshore tax evasion schemes and facilitators.

Box 2 illustrates the impact of VDP.

Box 2. **Examples of the impact of voluntary disclosure programmes**

Prior to its first AEOI exchanges in September 2017, South Africa launched a Special VDP which ran from 1 October 2016 to 31 August 2017. USD 1.8 billion worth of foreign assets were disclosed and the revenues gained amounted to USD 296 million. These are assets that were previously hidden off-shore by non-compliant taxpayers that will continue to contribute to tax revenue generation in the future. South Africa has also introduced a permanent VDP in its tax law, offering taxpayers to come forward on a voluntary basis to regularise their tax affairs. An amount of approximately USD 213 million was collected for the period from 1 April 2018 to 31 March 2019 under this programme. According to the South African Revenue Service, a large intake on VDP applications is in relation to foreign assets previously not disclosed.

The Voluntary Assets and Income Declaration Scheme launched in Nigeria from 1 July 2017 to 30 June 2019, grew the taxpayer database from 14 million in 2016 to 19 million in 2018 and yielded about USD 162 million.

Source: Global Forum Secretariat / OECD (2021), *Tax Transparency in Africa, Africa Initiative Progress Report 2020*, available at www.oecd.org/tax/transparency/documents/Tax-Transparency-in-Africa-2021.pdf.

Global Forum Secretariat / OECD (2020), *Tax Transparency in Africa, Africa Initiative Progress Report 2019*, available at www.oecd.org/tax/transparency/documents/Tax-Transparency-in-Africa-2020.pdf.

4.3. CORE PRINCIPLES OF VOLUNTARY DISCLOSURE PROGRAMMES

The design and implementation of a VDP will depend on the objectives of the programme and the national context where it is launched. However, a number of core principles and considerations should be observed to achieve an effective and successful programme (see Table 9).

4.4. HOW TO SET UP A SUCCESSFUL PROGRAMME?

4.4.1. Preliminary considerations

Before deciding on the terms and conditions of the programme, tax authorities should consider its effects on all taxpayers. A balance should be struck between attracting non-compliant taxpayers to come forward and not rewarding or encouraging transgressions. VDPs tread a fine line between:

- encouraging reluctant taxpayers to improve their behaviour
- retaining the support of the vast majority of already-compliant taxpayers.

If there is a perception that tax evaders are being offered better terms than people who declared all their income and offshore interests in the past, tax evasion rates might increase and the population will question the legitimacy of the programme. Carefully designed VDPs can benefit all stakeholders – taxpayers making

disclosures, compliant taxpayers and governments. The terms and conditions must be designed so that taxpayers who come forward voluntarily to join the programme:

- pay more than compliant taxpayers that fully disclosed offshore interests from the outset
- face less punitive sanctions than evaders that reject to comply with the programme and are later detected by tax authorities.

Creating a sense of urgency usually contributes to the success of a VDP set up in anticipation of CRS-AEOI exchanges. A jurisdiction should therefore seek to avoid repeatedly offering CRS-related VDPs within a short-time period.[42] Otherwise, the "last chance" warning will not be taken seriously. If VDPs are frequently rolled out, non-compliant taxpayers will dismiss the initiative in anticipation of another opportunity with better terms in the near future.

42. Permanent disclosure programmes are not addressed in this toolkit.

Table 9. **Core principles for a successful Voluntary Disclosure Programme**

1. Clarity on aims and terms	The terms of the programme must be clearly defined, published through guidance documents and communicated to taxpayers. All the consequences of the initiative (including on taxes, interests, penalties and criminal proceedings) should be openly informed. Communication must also focus on the aims of the programme, highlighting the benefits of engaging taxpayers with undisclosed offshore interests in a cost-efficient way with an eye on long-term sustainable compliance.
2. Balance between transparency and confidentiality	Transparency is essential to ensure the legitimacy and acceptance by compliant taxpayers of programmes that involve some degree of foregone interest payments and monetary penalties, in addition to protection from prosecution. The publication of the final impact of the programme is usually recommended, with the disclosure of costs and benefits of the programme. At the same time, the programme should ensure the confidentiality of all information disclosed by taxpayers joining the programme. Any doubt over the private character of the disclosure or fears of leaks will result in taxpayers opting out of the programme due to concerns about the publication of their financial affairs.
3. Consistency with the current compliance and enforcement regimes	A VDP should not be designed as an isolated programme without considering the impact it has on the broader compliance and enforcement framework. As a piece of a bigger puzzle, the VDP is one in a variety of actions that tax authorities can take as part of a comprehensive compliance strategy. If a broader perspective is not considered, VDPs may result in insufficient revenue collection and have a negative impact on other ongoing actions.
4. Help to deter further non-compliance	Successful disclosure programmes depend on taxpayers assuming that tax authorities have the tools, powers and capacity to deal with those that do not join the programme. Tax authorities should present VDPs as the last opportunity for regularisation under favourable terms before the implementation of the Standard, after which harsher penalties and prosecution guidelines should be applied to taxpayers that remain non-compliant and are detected.
5. Promote sustainable compliance of taxpayers with offshore interests	The success of the programme should not be measured only by the amount of joining taxpayers or revenue collected, but also by ensuring that taxpayers remain compliant in the long run. With the implementation of the Standard, taxpayers will be aware that undisclosed offshore interests are communicated between tax authorities, which serve as a solid deterrent for evasion in the future. The initiative must build on that and promote sustainable compliance as to offshore interests.

The more often VDPs are offered, the less additional revenue they are expected to generate. Recurring programmes may also reward taxpayers that dismissed the initial VDP and penalise those that joined it, impacting public trust in the system.

Where multiple VDPs are set up (e.g. a first short-term programme is launched at the time of the commitment followed by a second one closer to the date of the first exchange), the terms should be less generous in the successive programmes to create a sense of urgency as taxpayers can see that the opportunities for making a voluntary disclosure are steadily reducing, while the risks of detection are rising.

A jurisdiction implementing a CRS related VDP should therefore consider the following elements:

- A single VDP which sticks to its initial timeline (without further deadline extensions), the original terms and the last chance notice. Alternatively, a few successive VDPs with less favourable terms as the first exchange date approaches.
- Investing part of the collected revenue to fund the implementation of the Standard, with the received CRS data used to detect any remaining non-compliance.
- An increase in the severity of penalties and criminal prosecution for those that are detected by the tax authorities after rejecting the programme.

In addition to these initial considerations, tax authorities have multiple issues to consider for the design and implementation of a successful VDP.

4.4.2. Designing the programme

The VDP must be designed taking into account the legal framework of the jurisdiction and the overall objectives of the programme. Figure 8 presents a Design Tree that includes the main issues that policymakers must consider in the development of the initiative:

Scope of the programme

Policymakers should precisely determine the extent of the programme, including:

- which taxpayers can access it
- what taxes are covered
- its specific duration.

Other aspects relevant in the domestic context should also be considered in the definition of the scope of the programme. For instance, whether taxpayers having benefited from a previous VDP can qualify for the programme.

The limitation period or temporal restrictions normally applied to tax authorities (in tax audits or investigations) may determine the extent of assessment years that can be included in the programme in accordance with the domestic legal framework.

Terms and conditions

A central aspect of a VDP is the set of terms and conditions offered. The focus of policymakers should be to offer a balanced set of conditions, which often include foregoing some or all of the obligations and penalties normally applied to non-compliant taxpayers. At the same time, a clear message should be given that taxpayers who dismiss the initiative and are later detected will be handled firmly.

An internal dialogue within the tax authorities and with other relevant stakeholders (e.g. the Financial Intelligence Unit and the Public Prosecutor office) is recommended to ensure consistency with relevant rules in the non-tax space such as anti-money laundering rules. A jurisdiction may also consider setting up a joint team including all impacted authorities to ensure coherence and consultation during the design of the programme.

The main and most common incentives used in VDP are:

- a reduction in all or part of the interest charged on late payments and accrued during the overdue period
- a reduction in all or part of the penalties applied due to non-compliance, including late filing or late payments
- a waiver of prosecution related to administrative or criminal offences.

Voluntary disclosure programme

FIGURE 8. **Design tree for voluntary disclosure programmes**

Note: This figure relates to VDPs implemented in anticipation of the first CRS-AEOI exchanges. It is inspired by the decision tree developed in the following publication: OECD (2015), *Update on Voluntary Disclosure Programmes, A pathway to Tax Compliance, op. cit.*

The decision to reduce of interest and penalties and/or to waiver prosecution is related to the national context and objectives of the programme, which leads to a diverse set of conditions across different jurisdictions. Extended payment conditions for tax, interest and penalties owed are also often offered.

Reducing the tax rate or waiving taxes is not an approach generally recommended as it would constitute a kind of tax amnesty. It may lead to a more favourable treatment of non-compliant taxpayers than compliant taxpayers and negatively affect compliance rates in future.[43]

As most countries establish administrative and criminal offences in relation to tax evasion and concealing offshore assets, VDPs usually grant immunity from prosecutions in exchange for disclosure. The terms and conditions of the programme impact not only tax obligations, but also prosecutions or disclosure rules from other regulations (e.g. AML/CFT regulations). It is fundamental that the design of the VDP is done in consultation with other agencies and officials that operate in the affected areas, to prevent contradictory measures or the implementation of terms that weaken other active policies.[44] The scope of the protection from prosecution should be clearly defined. This protection may cover tax crimes and crimes related to remitting (or holding) assets offshore. However, if the untaxed income is the proceeds of another crime (e.g. corruption, drugs trafficking), the VDP should not confer immunity for these crimes.

Reporting requirements

Reporting requirements are critical to a successful VDP. They should define clearly the department of the tax authority in charge of collecting the applications, the method to be used for their submission, the set of information and documents (if any) to be reported (see Box 3).

The reporting method for the disclosure may vary from one jurisdiction to another. For instance, the

43. Bear, K., E. Le Borgne (2008), *Tax Amnesties, Theory, Trends and Some Alternatives*, International Monetary Fund, Washington, DC., p. 55, available at https://doi.org/10.5089/9781589067363.058.

44. The terms of a VDP should not imply exemption from AML/CFT obligations either on the part of persons subject to AML/CFT disciplines (banks, financial institutions, certain intermediaries, etc.) or on the part of the tax authority (see OECD (2015), *Update on Voluntary Disclosure Programmes, A pathway to Tax Compliance, op. cit.*).

Box 3. **Example of information and documents to be reported in a voluntary disclosure application**

The taxpayer applying for a VDP could be required to:

- correct all the tax returns for the non-barred period or file a specific form
- disclose all the undeclared accounts and assets held abroad or of which the taxpayer is the beneficial owner
- provide the precise and detailed origin of the assets held abroad, accompanied by any document proving this origin (e.g. certificate from the foreign Financial Institution justifying the origin of the funds transferred to the credited to the account when it was opened) or constituting a set of elements likely to establish this.
- provide a sworn statement that the returns or file submitted are sincere and covers all the undeclared accounts and assets
- provide a sworn statement that, to the taxpayer knowledge, no proceedings concerning the assets held abroad have been initiated to date, in any form whatsoever, by the tax authority or the judicial authorities
- provide all supporting documents relating to the amounts of foreign assets and income from these assets all over the period covered by the filing of amending tax return:
  - statements of assets or statements of wealth as at 1 January of each of the years or on 31 December of the previous year
  - annual statements of income issued by the foreign Financial Institution to justify the regularised income (dividends, interest, etc.)
  - annual statements of gains and losses drawn up by the foreign Financial Institution to prove the existence of gains (capital gains or losses)
  - if the foreign assets are held through an interposed structure (trust, foundation, company, etc.), all the legal documents relating to this structure (articles of association, incorporation contract, letter of intent, endorsements, deed of dissolution, etc.), the balance sheets and profit and loss accounts of the said structure, if they exist, for the period under review, and proof of any contributions made to the said structure and of any distributions received from it.

application to the VDP can be made on a prescribed paper or electronic form, a letter or an email, or a paper or electronic questionnaire. For instance, the submission could be done via the tax authority's website.

The deadline for the submission of the disclosure report and who is required to make the submission: the taxpayer or its legal representative, lawyer or accountant should also be reflected in the requirements

The tax authority should run a series of preliminary assessments of the reporting system, including ensuring the IT platform is tested and functional in advance of the submission of reports. Any unexpected issues on the website or disclosure form can result in failed attempts to join the programme.

Intelligence gathering

The VDP is an opportunity to gather information to identify other non-compliant taxpayers as well as professionals that promote offshore evasion. The intelligence collected can help identify schemes used by tax evaders and what accessible information is relevant to tax auditors, securing long-term benefits by building the tax authority's knowledge on non-disclosure.

For instance, intelligence provided on foreign Financial Institutions frequently used by taxpayers or on international law firms that design tax evasion schemes can lead to more targeted tax audits through international cooperation.

Therefore, the tax authority should consider what information it should collect through the VDP and make it a condition to qualify to the programme (e.g. providing all required documents and information on foreign accounts, assets, institutions and facilitators).[45]

Communication

The communication strategy is fundamental to draw attention and interest to the programme. As creating early awareness is key for the success of VDPs, active public engagement should start well in advance of the launch date. It is important to clearly communicate on conditions and objectives to all taxpayers but also to accounting and legal professionals advising taxpayers.

The objective is dual: (i) encourage and attract non-compliant taxpayers to participate in the programme and (ii) create an understanding of the programme by compliant taxpayers and avoid it creating perceptions of unfairness that will adversely affect compliance.

Communication towards non-compliant taxpayers

Non-compliant taxpayers are interested in all the details and consequences of joining the programme. Therefore, making a clear and broad communication strategy towards them should be a priority. The divulgation of the terms and conditions of the programme can be carried out in multiple forms, including official documents, media releases and others. VDP information should be made available on the tax authority website.

Developing a technical guidance document for professional bodies associated within the financial industry – including tax accountants, lawyers, trust and company service providers and corporate federations – ensures that all relevant stakeholders are informed of the details of the programme. Organising meetings with these professionals should be considered. Establishing a central point of contact that can be approached by taxpayers or advisors on an anonymous base for initial discussions also increases confidence on the programme.

Communication towards compliant taxpayers

As VDPs often involve the waiver of obligations and penalties, compliant taxpayers at first may consider the programme unfair. If the details and objectives of the programme are not properly explained, some might conclude that non-compliance is being rewarded. The communication strategy plays an important role by creating awareness of the programme and its objectives, outlining the negative impact of tax evasion in public coffers and how VDPs have the potential to address deep-rooted irregularities and increase revenue collection. The VDP could for instance be explained in mass media.

4.4.3. Implementing the programme

In addition to the design of the VDP, there are a number of practical issues to be considered when tax authorities are contemplating the actual implementation of the programme.

45. Providing information on facilitators should be balanced against the objective of the VDP (i.e. attracting non-complaint taxpayers) as these intermediaries may discourage their clients to adhere to the programme.

Organisation

The organisational structure of the tax authority conditions the practical implementation of a VDP. Implementing the programme in a centralised administration is not the same as in a federalised or decentralised structure.

Best practice points to the implementation of a specialised unit or team (Disclosure Unit) to centrally manage the data from a single location with additional confidentiality rules in place. A separate unit ensures that the information collected is not widely shared within the tax authority, reducing the possibility of data leaks.

For federal jurisdictions with tax powers shared between different entities, concentrating the VDP functions in the central authority ensures uniformity in the treatment of applicants and increases public confidence in the confidential handling of the data.

A decentralised approach may also be followed provided that confidentiality, consistency and efficiency are ensured. The local or regional offices should be able to provide information about the programme and address questions of the taxpayers. This approach may involve additional costs.

In any cases, the organisational structure and the infrastructure used must ensure that the information is safely stored.

An early estimation of the number of taxpayers expected to join the programme will also provide officials with a projection of the financial, human and organisational resources that need to be invested in the VDP for its adequate operation.

Timeline

As the implementation of the Standard in a jurisdiction changes the landscape of offshore secrecy to its tax residents, the best period to launch a VDP is in the years before CRS-AEOI becomes operational. Taxpayers are faced with a clear scenario of elevated detection risks and realise the VDP is a unique opportunity to address any issues under favourable conditions.

Due to the technical complexities of the disclosure and to offer taxpayers time to consider all details with advisors and prepare a submission report, communication campaigns on the VDP should start in advance of the launch date. This will create early awareness and allow for initial preparations.

As for the timeline of the programme itself, an extended period should be prioritised – ideally comprising of one or more years – terminating in advance of the initial round of CRS collection and exchange by the jurisdiction. For instance, if a jurisdiction commits in 2022 to AEOI implementation by 2025, the VDP could be launched still in 2022 and expire by the end of 2024.

Confidentiality

Confidentiality is a major concern for non-compliant taxpayers. The potential reputational damage from the publication of personal tax affairs prevents many taxpayers from joining a VDP. The risk of leaks to other government agencies is also a concern. The programme and the communication strategy must reassure taxpayers of these concerns, placing privacy and confidentiality as central pillars of the programme.

Besides following all standard legal obligations regarding confidentiality, additional measures can be taken to ensure privacy and increase the confidence of taxpayers. These include limiting access to the information to designated tax officials in a separate specialised unit, or enacting additional tax secrecy provisions.[46] In federal jurisdictions with a decentralised tax system, restricting the information from being shared to other agencies at regional or municipal level also prevents data leaks.

Assessment

The assessment of the efficiency and success of the VDP is an important part of the programme. While the immediate impact can be measured by the number of taxpayers that join the programme and the revenue declared, it is also important to measure the long-term deterrent impact of the VDP over the disclosure of offshore assets.

Sustained compliance can be assessed through annual disclosure obligations required from all taxpayers with offshore interests. A periodical assessment of the number of taxpayers with offshore assets can reflect the

46. Whether the public prosecutor office can request information covered by the VDP could also be a key consideration for the jurisdiction, as it could discourage taxpayers from joining the programme.

impact of the programme years after its conclusion, as seen in Brazil's VDP experience (see Box 4).

4.4.4. Recommended legislation content and country experience

A VDP should be enacted through a legal initiative, such as a law or an executive decree. While each jurisdiction has its own legislative procedures and particularities, a range of basic topics must be addressed through the legislation to ensure the successful implementation of the programme. These basic elements include:

- preamble mentioning the constitutional basis and the legislative and regulatory provisions in effect for the collection of revenue from taxpayers through tax compliance
- establishment of the programme based on the objective of promoting voluntary compliance in relation to undisclosed offshore interests
- scope of the programme, with a clear list of the taxes covered by the programme, which taxpayers may benefit from it and which are excluded from joining (i.e. with previous convictions of tax evasion, currently under investigation for tax offences, or who have already benefited from a VDP in the past)
- types of asset and income which are included in the programme and those that are excluded from it (i.e. income or assets derived from illicit activities), with rules on how to determine the value of the offshore assets to be disclosed
- assessment years which are included in the programme (considering statute of limitation periods), which possibly include the obligation for taxpayers to amend tax declarations from previous years
- terms and conditions of the VDP, including the interests and penalties to be applied during the programme, as well as any form of immunity or exemption from prosecution
- consequences of not complying with the programme, including liability to additional compliance actions, harsher penalties and updated prosecution guidelines
- reporting requirements, including how interested taxpayers can submit their declaration, the basic information it will require and any requirements on documents or records to be provided
- terms of confidentiality and data treatment applied to the information provided by taxpayers
- Indication of the government body empowered to publish regulations on the programme, including technical guidance documents, further details and clarifications.

The points mentioned above should be considered as general topics and issues to be addressed in the VDP legislation. For additional recommendations and the provision of tailored comments to a particular national context, the Global Forum Secretariat is available to assist jurisdictions.

Table 10 illustrates the different characteristics and effectiveness of VDP across multiple jurisdictions.

Box 4. **Assessment of programme efficiency in Brazil**

The Central Bank of Brazil requires all resident taxpayers with offshore interests to submit a periodical declaration called the Brazilian Capital Abroad. With the implementation of a VDP in Brazil, the number of respondents to the survey greatly increased in the period. From 30 600 taxpayers submitting the declaration in 2013 before the programme was launched, 2014 received reports from 55 200 taxpayers. Out of the 24 600 new respondents, 21 200 had joined the disclosure programme with a total value of USD 54 billion in disclosed assets.

From 2014 to 2019, the number of respondents further increased from 55 200 to 65 500. The strong increase in compliance and the maintenance of those new respondents over the following years is a positive reflection of the efficiency of the programme and its long-term impact against offshore tax evasion.

Source: Federal Revenue Service of Brazil and Central Bank of Brazil, Direct Investment Report, available at www.bcb.gov.br/publicacoes/relatorioid/RelatorioID2019, pp. 52-53.

Table 10. **Voluntary disclosure programme - Selection of country experiences**

Brazil
Prior to commencing CRS exchanges in September 2018, Brazil launched the Special Asset Regularisation Regime (RERCT - *Regime Especial de Regularização Cambial e Tributária*) in January 2016. The RERCT gave Brazilian tax residents a 210-day window of opportunity to voluntarily report to the tax authorities all assets, rights and resources (originated from licit activities) that had either been wrongfully reported or not previously reported. Taxpayers joining the programme were required to amend their tax returns for 2014, 2015 and 2016 to reflect the newly disclosed amounts The terms and conditions of the programme established a 15% tax rate and penalties of 100% of the tax owed. Some criminal proceedings were also waved for taxpayers joining the programme. The full payment of taxes and penalties can result in the regularisation of the taxpayer if the Federal Tax Authority does not identify non-compliance issues within 5 years from the declaration year. The programme was not available to politicians and public officials, as well as their close relatives, in addition to persons convicted of tax crimes. The programme legislation guaranteed secrecy of the process through tax confidentiality standards. Information disclosed could not be shared by the Federal Tax Authority with other public agencies or departments. The information cannot be shared with the State and Municipal Tax Administrations. Notwithstanding, it can be shared with the Public Ministry and the Justice on request or as a result of the tax proceedings. The adherence to RERCT resulted in around EUR 10 billion collected (in taxes and fines) in 2016. In 2017, a second voluntary disclosure programme (RERCT 2) was launched with an increased penalty rate of 135%, which resulted in the collection of approximately EUR 0.5 billion in 2017, the same year that Brazil started collecting CRS information to be exchanged from 2018.
France
In 2013, France established a Voluntary Disclosure Programme aimed at the regularisation of undisclosed offshore assets. In effect from 2014 to 2017, the programme was timed to offer taxpayers an opportunity to come forward before the initial exchange of CRS data upon the implementation of AEOI on 1 September 2017. By application of the ordinary tax procedure law, the programme involved payment of all taxes due and covered a 10-year limitation period for undeclared financial assets such as offshore bank accounts. As the programme considered the fact that taxpayers came to the disclosure on voluntary basis, the percentage of the penalty was either 15% or 30% (either 25% or 35% from 14 September 2016) dependent on the behaviour of the taxpayer. The Ministry of Public Action and Accounts instituted a specialised separate disclosure unit (STDR – *Service de Traitement des Déclarations Rectificatives*) to manage the high volume of submissions, which generated results beyond the original expectations of the programme upon its dissolution in 31 December 2017. From 2014 to 2017, 53 000 declarations were submitted by taxpayers regarding EUR 35 billion in regularised assets, resulting in the collection amounting to about EUR 10 billion in revenues.
India
In 2015, India launched the Black Money (Undisclosed Foreign Income and Assets) and Imposition of Tax Act. As part of the Act, a VDP designed to cover the non-disclosure of offshore income and assets held by Indian taxpayers was offered from 1 July 2015 to 30 September 2015.The person availing the benefit of this window of disclosure had to pay a tax at 30% of the undisclosed foreign income and asset along with equivalent amount of penalty. While the Act did not grant full immunity from prosecution, it established that the declaration itself is not admissible as evidence against the declarant – an approach that leaves room for prosecution if other evidence is made available to the government. To highlight the unique opportunity of the programme and provide a stricter treatment for taxpayers that did not join the initiative, the Act increased the penalty in respect of undisclosed foreign income and asset to 90% - in addition to the 30% tax rate. The Act also established harsher criminal sanctions for different offences related to tax evasion and non-disclosure of offshore interests, possibly resulting in up to ten years of imprisonment. The strict approach from the Indian government to taxpayers after the VDP time window reflected the implementation of CRS-AEOI in 2017, which increased the capacity of the tax authorities to detect offshore tax evasion.

Voluntary disclosure programme

Kenya

The Finance Act 2020 established a VDP in effect from 1 January 2021 to 31 December 2023. The programme covers undisclosed or unpaid amounts accrued from 1 July 2015 to 30 June 2020. As an incentive for taxpayers to adhere to the programme at an early stage, the relief on penalties and interest is gradual: relief is granted at 100% for disclosures made in 2021, 50% for disclosures made in 2022 and reduced to 25% for disclosures made in 2023. The program allows for taxpayers to settle the principal tax, while obtaining the benefit from relief in respect of the resulting penalties and interest and shall not be prosecuted in respect of undisclosed tax liabilities. The programme is not available to taxpayers currently under investigation, audit procedure or active judicial litigation with the tax authorities related to the tax liability to be disclosed.

Malaysia

As part of the 2019 Malaysian Budget, the Minister of Finance established the Special Voluntary Disclosure Programme (SVDP) in effect between November 2018 and September 2019. The Malaysian SVDP utilised a gradual penalty rate based on the date of the adhesion of the taxpayer to the programme and the payment of the owed amounts: for declarations made until June 2019 with payment until 1 July, a penalty rate of 10% applies; for declarations between July and September 2019 with payment until 1 October, the penalty rate is increased to 15%. If a taxpayers does not adhere to the SVDP and is posteriorly detected by the tax authority, penalty rates apply at rates between 45% and 300%.

In 2021, in response to reports of audits and investigations of taxpayers that disclosed information through the SVDP, the Revenue Board of Malaysia released a statement highlighting that further compliance actions were being directed at taxpayers suspected of not disclosing all taxable income in their declarations, therefore not complying with the conditions of the programme.

United Kingdom

The United Kingdom developed as part of the 2017 (n°2) Finance Act a programme entitled Requirement to Correct (RTC) towards taxpayers with undisclosed offshore tax. In effect from 6 April 2017 until 30 September 2018, this programme differs from the other examples mentioned above as it did not extend beneficial conditions to attract taxpayers. The RTC in fact created an obligation for taxpayers to disclose their situation before 1 October 2018, when much harsher penalties came into effect under the Failure to Correct (FTC) regime.

While penalties of 30% of the tax due typically applied before 30 September 2018, any disclosure or detection of undeclared offshore interests after October 2018 were subject to the FTC regime, resulting in penalties between 100% and 200% of the amount owed – minimum penalties set at 150% for prompted disclosure (following early detection by the tax authorities) and 100% for spontaneous disclosures – in addition to the tax owed and corresponding interest.

The RTC and FTC regimes were scheduled around the date of the initial CRS exchanges from AEOI implementation, with the United Kingdom adopting a policy of escalating penalties to highlight the increased risk from continued non-compliance.

5. International legal framework

One of the building blocks for jurisdictions to be able to exchange information under the Standard is to have an international legal framework in place that allows for the automatic exchange of information with partner jurisdictions.

All implementing jurisdictions rely on the MAAC[47] supplemented by the CRS MCAA, which operationalises the exchanges. The multilateral approach has proven to be the most efficient route to put in place widespread networks of exchange relationships:

- This approach allows jurisdictions to easily and more efficiently activate relationships with all interested appropriate partners and to exchange information with them as required by the Standard.
- It favours the level playing field, by putting in place an extensive exchange relationship network to prevent taxpayers from moving their assets to avoid information on their offshore activities being reported to their jurisdiction of tax residence.

Alternatively, jurisdictions can also establish automatic exchange relationships under bilateral tax treaties, although this route only plays a minor role in the context of the implementation of the Standard and would rely on the existing CRS jurisdictions negotiating each agreement on a bilateral basis.

This part of the toolkit focuses on the multilateral approach using the combination of the MAAC and the CRS MCAA.

5.1. THE CONVENTION ON MUTUAL ADMINISTRATIVE ASSISTANCE IN TAX MATTERS

The MAAC is a multilateral treaty aimed at assisting jurisdictions to better enforce their laws, providing an international legal framework for exchanging information and co-operating in tax matters with a view to countering international tax evasion and avoidance.

It was developed jointly by the OECD and the Council of Europe (CoE). Countries that are not members of either the OECD or the CoE can request to be invited to join the MAAC. By becoming a Party to the MAAC, a country significantly and rapidly expands its administrative co-operation framework. The Global Forum has developed a toolkit to assist countries aspiring to become

47. As amended by the 2010 Protocol.

a Party to the MAAC which provides more details on the benefits it entails.[48]

The MAAC has become the most used global instrument for multilateral co-operation in EOI and other forms of administrative assistance in tax matters. More than 140 jurisdictions are participating in the MAAC.[49]

Pursuant to its Article 6, two or more Parties can mutually agree to automatically exchange predefined foreseeably relevant information in accordance with the procedures determined by the Parties by mutual agreement. This provision provides the legal basis for AEOI. The operationalisation of this provision requires administrative agreements to determine, in particular, the information to be automatically exchanged and the time and method of the exchanges.

Regarding CRS-AEOI exchanges, a specific multilateral CAA has been developed – the CRS MCAA – which supplements the MAAC and derives its legal force from it.

5.2. THE MULTILATERAL COMPETENT AUTHORITY AGREEMENT ON AUTOMATIC EXCHANGE OF FINANCIAL ACCOUNT INFORMATION

Under the legal basis provided by Article 6 of the MAAC, the CRS MCAA was developed to operationalise exchanges under the Standard. The CRS MCAA contains specific provisions that set out detailed procedures regulating the modalities of the exchanges taking place every year on an automatic basis.

The CRS MCAA[50] is structured as follows:

- a declaration to be signed by the competent authority of the jurisdiction
- a preamble with recitals explaining the purpose of the CRS MCAA and explaining its provisions
- eight sections containing the agreed provisions of the CRS MCAA
- six annexes containing the notifications required for the CRS MCAA to enter into effect for a competent authority.

All the provisions of the CRS MCAA are in English and French, both texts being equally authentic.

More than 110 jurisdictions (i.e. all implementing jurisdictions) are signatories of the CRS MCAA,[51] allowing for a broad network of around 7 500 relationships.[52]

This section explains the main sections of the CRS MCAA and provides guidance on the steps that must be completed to become a signatory and to activate relationships under it.

5.2.1. Overview of the provisions of the Competent Authority Agreement on Automatic Exchange of Financial Account Information

Definitions

Section 1 of the CRS MCAA introduces the definitions of the terms relevant to its application. In particular, it clarifies that:

- "CRS" means the Standard developed by the OECD with G20 countries. The Commentaries are expressly included in the definition.
- "Jurisdiction" refers to a country or a territory in respect of which the MAAC is in force either through ratification (MAAC, Art. 28) or territorial extension (MAAC, Art. 29).
- "Competent Authority" is the persons and authorities listed as competent authority in the Annex B of the MAAC.

Information to be exchanged and form of the exchanges

Section 2 of the CRS MCAA sets out the terms under which the exchange of information is to take place between competent authorities and the information that is to be exchanged.

48. Global Forum Secretariat / OECD (2020), *A Toolkit for Becoming a Party to the Convention on Mutual Administrative Assistance in Tax Matters*, available at www.oecd.org/tax/transparency/documents/MAAC-toolkit_en.pdf.

49. A chart of participating jurisdictions to the MAAC is available at www.oecd.org/tax/exchange-of-tax-information/Status_of_convention.pdf.

50. The text of the CRS MCAA is available at www.oecd.org/tax/automatic-exchange/international-framework-for-the-crs/multilateral-competent-authority-agreement.pdf.

51. The list of signatories of the CRS MCAA is available at www.oecd.org/tax/automatic-exchange/about-automatic-exchange/crs-mcaa-signatories.pdf.

52. The list of signatories of the CRS MCAA is available at www.oecd.org/tax/automatic-exchange/international-framework-for-the-crs/exchange-relationships.

It provides that competent authorities will annually and automatically exchange information obtained pursuant to the reporting and due diligence rules set out in the CRS with other competent authorities with respect to which the CRS MCAA is in effect.

Exchanges can be:

- Reciprocal - i.e. the competent authority will send CRS data to the competent authorities of its partner jurisdictions and will in turn receive the same from them.

- Non-reciprocal - i.e. the sending competent authority will not receive CRS data from the competent authorities of its partner jurisdictions.

  A jurisdiction will typically be non-reciprocal in one of two situations: (i) the jurisdiction does not need CRS data for tax purposes (e.g. the jurisdiction does not have a direct tax system) and therefore will permanently exchange on a non-reciprocal basis; (ii) the jurisdiction wishes to exchange on a reciprocal basis but has been assessed by the Global Forum as not reaching the appropriate level of confidentiality and data safeguards for handling exchanged data due to serious weaknesses in its overall confidentiality and data safeguards framework. In the latter case, the jurisdiction is invited to temporarily exchange on a non-reciprocal basis during the time needed to fix such weaknesses, provided that the confidentiality and security of its specific arrangements to collect domestic data and send it to exchange partners are sufficient. In practice, the non-reciprocity is materialised by filing the notification foreseen in Section 7(1)(b) of the CRS MCAA (see Table 11).

Section 2 also lists the information to be exchanged. These are the same as the identification and Financial Account information provided in the CRS (Section I, paragraph A).[53] More details and explanations on the information to be reported can be found in Chapter 5 of the Implementation Handbook.

Time and manner of the exchanges

Section 3 of the CRS MCAA outlines the timelines and manner in which exchanges of information are to take place.

First, it clarifies that CRS data is to be exchanged between two competent authorities commencing from the calendar year for which the CRS MCAA has effect. Where a jurisdiction's tax year diverges from the calendar year, attention must be paid to the date of effect of the MAAC (see Subsection 5.3.2 of the toolkit).

Second, information is to be exchanged within nine months after the end of the calendar year to which the information relates, i.e. September following the year the information is collected. For example, if a competent authority is to exchange information related to the reportable year 2021, the information can be exchanged at any time between January 2022 and September 2022.

Jurisdictions should consider these timelines when defining their internal dates for reporting (i.e. the date when Reporting Financial Institutions are required to send the information to the competent authority), considering also the time needed to sort, prepare and validate the information that will be exchanged with partner jurisdictions. Jurisdictions would usually require two to four months to finalise these procedures once the information has been received in order to have the information ready to be exchanged. The reporting date set by jurisdictions is usually May or June in the year after the information is collected, allowing sufficient time for the competent authority to sort and prepare the information before transmitting it by end of September in that year.

Finally, jurisdictions must exchange the CRS data in the CRS XML schema and agree the method of transmission that will be used with each exchange partner. In order to maximise standardisation and security and minimise complexities and costs, the CTS was developed by the OECD (see Section 7.2 of the toolkit). The CTS is the secure transmission method used by all committed jurisdictions that have started CRS-AEOI exchanges.

Collaboration on compliance and enforcement

Section 4 of the CRS MCAA establishes an effective collaboration between the receiving and sending competent authorities to ensure compliance with, and enforcement of, the reporting and due diligence requirements. The receiving competent authority is required to notify the sending competent authority where it has reason to believe there is (i) an error in the information received or (ii) non-compliance by a Reporting Financial Institution.

53. However, the exception provided in the Section I, Paragraph F of the CRS allowing for a phase-in of the exchange of the total gross proceeds from the sale or redemption of Financial Assets is not applicable in the context of the CRS MCAA.

Confidentiality and data safeguards

Section 5 of the CRS MCAA relates to confidentiality and data safeguards. It provides that the information exchanged must be subject to:

- the confidentiality provisions and other safeguards provided for in the MAAC, in particular its Article 22
- the safeguards that are required under the domestic law of the sending jurisdiction which are specified in Annex C of the CRS MCAA relating to specified data safeguards.

In the event of termination of the CRS MCAA, this obligation continues to apply for all information previously received under the CRS MCAA (see CRS MCAA, Section 7).

Section 5 creates an obligation on the competent authorities to notify the Co-ordinating Body Secretariat (CB Secretariat) immediately of (i) any breach of confidentiality or failure in the data safeguarding arrangements and (ii) any sanction and remedial actions consequently imposed. This obligation will allow the CB Secretariat to notify exchange partners.

The Global Forum has developed specific guidance for jurisdictions on putting in place appropriate data breach management procedures, including dissemination mechanisms to keep relevant stakeholders such as the CB Secretariat and exchange partners informed of the situation where required. This guidance is available to competent authorities upon request. Some guidance on data breach management is also contained within the Confidentiality and Information Security Management Toolkit.[54]

Consultations and Amendments

Section 6 of the CRS MCAA refers to the consultation and amendment procedures:

- In case any difficulties in the implementation or interpretation of the CRS MCAA arise, the concerned competent authorities may consult one another to develop measures to ensure the terms of the CRS MCAA are fulfilled. In that case, the CB Secretariat shall be notified of the agreed measures so that it can inform the other competent authorities which have not participated in the consultations.
- The procedure to amend the CRS MCAA can be amended by consensus by written agreement of all the competent authorities for which it is in effect.

Term of the CRS MCAA

Section 7 details the rules relating to the terms of the CRS MCAA.

Notifications

Section 7 lists the notifications that the competent authority of a jurisdiction must lodge with the CB Secretariat before the CRS MCAA can take effect with another jurisdiction (i.e. to be able to activate a relationship with a partner to exchange information under the Standard).

Table 11 provides more detailed explanations on each one of the six notifications. Templates for these notifications can be provided to competent authorities by the CB Secretariat (cb.mac@oecd.org).

These notifications are to be lodged at the time of signature of the CRS MCAA or as soon as possible after the signature. The CRS MCAA will not be in effect with another jurisdiction until these notifications have been properly lodged. These notifications must be signed by the competent authority of the jurisdiction as notified in Annex B of the MAAC. They remain valid until the CB Secretariat is notified of any modifications.

Jurisdictions exchanging information for the first time will need to consider this when looking to activate relationships with other jurisdictions.

Date of effect

The CRS MCAA can be signed by the competent authority of a jurisdiction while the MAAC is not yet in force and in effect. Therefore, a jurisdiction which has only signed or expressed its intention to sign the MAAC, can sign the CRS MCAA. However, the MAAC must be in force and in effect and all the required CRS MCAA notifications lodged for the CRS MCAA to take effect.

Therefore, Section 7 sets out the date of effect of the

54. Global Forum Secretariat / OECD (2020), *Confidentiality and Information Security Management Toolkit*, op. cit.

CRS MCAA between two competent authorities, which is the later of the following dates:

- the date on which the second of the two competent authorities lodges the required notifications,
- the date on which the MAAC is in force and in effect for both jurisdictions.

Suspension and termination

Pursuant to Section 7 of the CRS MCAA, the competent authority of a jurisdiction may suspend its exchanges with another competent authority or terminate its participation to the CRS MCAA.

- **Suspension**: the suspension of the CRS MCAA may be triggered where the competent authority of a jurisdiction has determined that there is or has been significant non-compliance by another competent authority with the provisions of the CRS MCAA.

  Significant non-compliance includes, but is not limited to, non-compliance with the confidentiality and data safeguard provisions, a failure to provide timely or adequate information as required under the CRS MCAA.

  The suspension must be notified in writing to the other CA and it has immediate effect.

- **Termination**: the competent authority of a jurisdiction may terminate its participation in the CRS MCAA, or with respect to a particular competent authority, by giving notice of termination in writing to the CB Secretariat. The termination will take effect on the first day of the month following the expiration of a period of 12 months after the date of the notice of termination.

The Co-ordinating Body Secretariat

Section 8 relates to the CB Secretariat which is in charge of notifying all competent authorities of the CRS MCAA notifications it has received and all signatories on the signing of the CRS MCAA by a new competent authority.

This Section also provides that all signatories share equally, on an annual basis, the costs for the administration of the CRS MCAA. However, jurisdictions that qualify for the flat *de minimis* fee of the Global Forum and have an annual GDP per capita that does not exceed the world average GDP per capita as published by the World Bank are exempted from sharing the costs.[55]

5.2.2. Signing and activating the Multilateral Competent Authority Agreement on Automatic Exchange of Financial Account Information

Signing the Multilateral Competent Authority Agreement on Automatic Exchange of Financial Account Information

To become a signatory of the CRS MCAA, the competent authority of the jurisdiction or its designated representative shall sign the Declaration,[56] which is attached to the CRS MCAA, and provide the Annex F notification which details the intended exchange dates which must be deposited at the time of signature.

To initiate the signing of the CRS MCAA, a jurisdiction is invited to contact by email the CB Secretariat (cb.mac@oecd.org), which will prepare a package for signature. The jurisdiction would need to provide to the CB Secretariat:

- the name and title of the signatory of the Declaration[57]
- the intended signing date
- the Annex F notification filled with the intended exchange dates.

The CB Secretariat will then provide the jurisdiction with the CRS MCAA package for signature.

The CRS MCAA is usually signed remotely in the jurisdiction by the competent authority. The signed package shall be dispatched to the OECD via diplomatic channels. It is also recommended to send a PDF scan to the CB Secretariat (cb.mac@oecd.org).

Once the original package is received, the CB Secretariat will acknowledge receipt through a *procès-verbal*, confirming that the competent authority of the jurisdiction is then a signatory to the CRS MCAA.

55. Article X of the Rules of Procedure of the CB of the MAAC.

56. The text of the CRS MCAA is available at www.oecd.org/tax/automatic-exchange/international-framework-for-the-crs/multilateral-competent-authority-agreement.pdf.

57. The competent authority listed in Annex B of the MAAC should communicate the name and title of the person who will sign the Declaration. The Declaration must be signed by the competent authority or by someone with the authority to represent it.

Table 11. **Notifications pursuant to Section 7 of the CRS MCAA**

Paragraph of Section 7	Element(s)	Explanation
Section 7(1)(a)	Legislation and due diligence deadlines	The competent authority of the jurisdiction needs to notify and provide the CB Secretariat with the domestic law, regulations and or guidance implementing the CRS and under which its Reporting Financial Institutions shall collect and report the required information to its competent authority. Jurisdiction must also notify the effective dates for the due diligence and reporting as follows: ● Date from which an account opened with a Reporting Financial Institutions is considered a New Account and when the information related to these accounts is expected to be exchanged for the first time. ● Date until which an account opened with a Reporting Financial Institutions is considered a Preexisting Account and when the information related to these accounts is expected to be exchanged for the first time, differentiating among Individual High Value Accounts, Individual Lower Value Accounts and Entity Accounts.
Section 7(1)(b)	Non-reciprocity	The competent authority of the jurisdiction needs to confirm whether it will exchange information on a non-reciprocal basis. This covers two situations: ● The competent authority of the jurisdiction does not need CRS data for tax purposes (e.g. the jurisdiction does not have a direct tax system). ● The competent authority of the jurisdiction does not meet an appropriate level of confidentiality and data safeguards. In that case, the jurisdiction is invited to temporarily exchange on a non-reciprocal basis (provided its framework is found adequate to do this), the time to fix any deficiencies relating to its confidentiality and data safeguards framework.
Section 7(1)(c)	Transmission and encryption method(s)	The competent authority of the jurisdiction needs to state the method by which it intends to transmit the information to other competent authorities. All jurisdictions use the CTS.
Section 7(1)(d)	Protection of personal data	The competent authority of the jurisdiction needs to specify whether it has any safeguards for the protection of personal data under its domestic legislation to which all information exchanged shall be subject. Any specification will be additional to the confidentiality rules and other safeguards provided for in the MAAC.

Paragraph of Section 7	Element(s)	Explanation
Section 7(1)(e)	Confidentiality rules and data safeguards	There are two versions of this notification. ● For jurisdictions that have completed the confidentiality and data safeguards assessment by the Global Forum, a notification whereby the competent authority of the jurisdiction states that it has in place the required confidentiality and data safeguards requirements. It also has to attach the completed confidentiality and data safeguards questionnaire and refer to its completed confidentiality and data safeguards assessment report. ● For jurisdictions for which the assessment of the confidentiality and data safeguards arrangements resulted in recommendations to address serious gaps identified, or for which the assessment process has not yet concluded, an alternative notification acknowledging that they will exchange information on a temporary non-reciprocal basis and confirming that they have adequate measures to ensure the required confidentiality and security in respect of the specific arrangements to collect and send information to other jurisdictions. The completed confidentiality and data safeguards questionnaire also has to be attached.
Section 7(1)(f)	Intended Exchange Partners	The competent authority of the jurisdiction needs to list all other jurisdictions with respect to which it intends to have the CRS MCAA in effect, i.e. the list of jurisdictions with which it intends to exchange information. This list is commonly referred to as the list of intended exchange partners. The competent authority of the jurisdiction shall list all Interested Appropriate Partners.

Relationships activated under the Multilateral Competent Authority Agreement on Automatic Exchange of Financial Account Information

While the CRS MCAA is a multilateral agreement, it creates only bilateral relationships through an activation process. A CRS-AEOI relationship will be activated with another jurisdiction provided that both jurisdictions have:

- the MAAC in force and in effect
- lodged the required CRS MCAA notifications with the CB Secretariat
- incorporated each other in their list of intended exchange partners (i.e. notification pursuant to Section 7(1)(f)).

All activated relationships are reflected on the Automatic Exchange Portal,[58] which shows whether:

- relationships are activated in either direction (i.e. to receive and/or to send information) as some jurisdictions proceed to non-reciprocal exchanges
- a relationship is activated although the CRS MCAA is not immediately in effect. In these cases, a clarification on the date from which the CRS MCAA is in effect is made. For example, the following comment "*CRS MCAA activated - Effective for taxable periods starting on or after 01 January 2020*" means that the first exchanges under the Standard will take place by September 2021, with respect to the tax year 2020.

5.3. INTERACTION BETWEEN THE CONVENTION ON MUTUAL ADMINISTRATIVE ASSISTANCE IN TAX MATTERS AND THE MULTILATERAL COMPETENT AUTHORITY AGREEMENT ON AUTOMATIC EXCHANGE OF FINANCIAL ACCOUNT INFORMATION

Where a jurisdiction which committed to implement the Standard by a specific date does not yet have the MAAC in effect, that jurisdiction should take into consideration

58. www.oecd.org/tax/automatic-exchange/international-framework-for-the-crs/exchange-relationships.

the interaction between the MAAC and the CRS MCAA to ensure that it can start its first exchanges as intended.

The date of effect of the CRS MCAA is linked to the date of effect of the MAAC. Therefore, the committed jurisdiction should ensure that the MAAC will have taken effect for the calendar year for which it intends to start its first exchanges. For instance, if a jurisdiction intends to exchange information in September 2022 with respect to the calendar year 2021, it should have the MAAC in effect for the full calendar year 2021.

Therefore, two elements must be taken into consideration by the committed jurisdiction:

- The date of effect of the MAAC depends on the deposit of the ratification instrument by the jurisdiction.
- Whether the tax year applicable in the jurisdiction differs from the calendar year.

5.3.1. Date of effect of the Convention on Mutual Administrative Assistance in Tax Matters

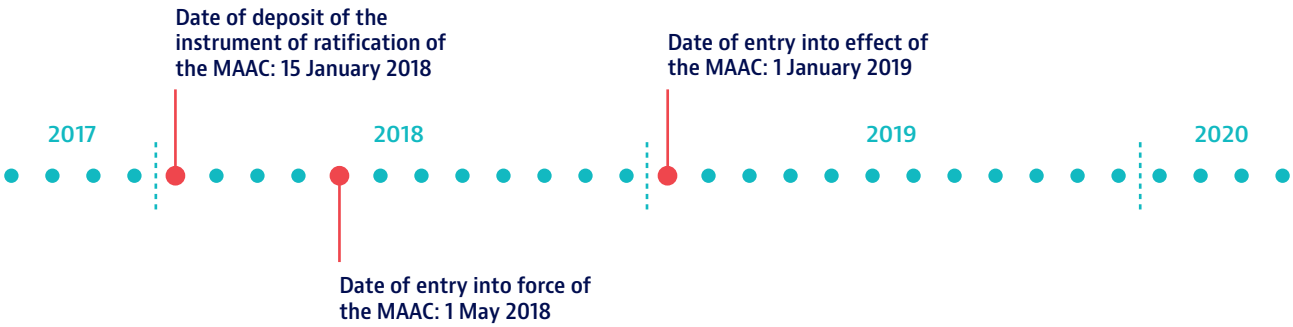
Due to the procedures and timelines required for the MAAC to be in force and in effect, some planning is required to ensure that all the formalities are completed in due time for the first exchanges to start as intended.

The MAAC enters into force on the first day of the month following a period of three months after the date of deposit of the instrument of ratification from a Party. It takes effect for taxable periods starting on or after 1 January of the year following the one in which the MAAC entered into force in respect of a Party (MAAC, Art. 28).

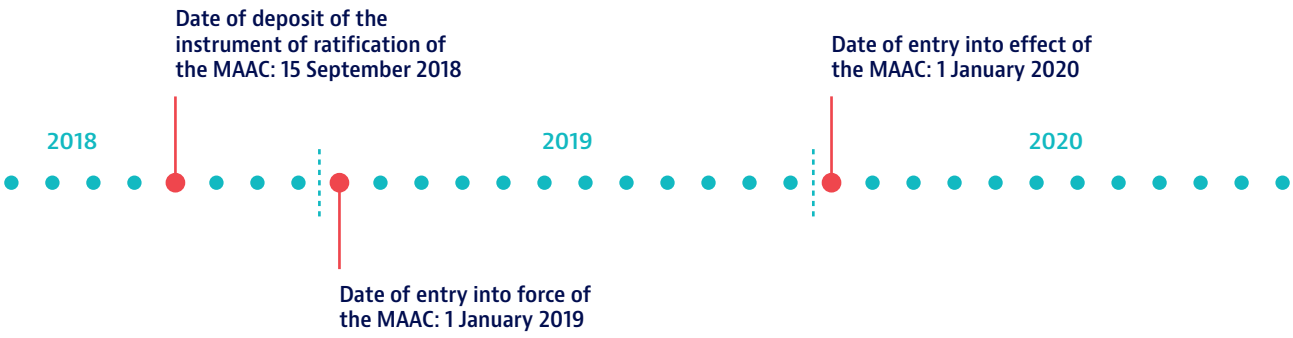
Figure 9 illustrates the impact of the date of the deposit of the ratification instrument of the MAAC on its entry into force and its date of effect. In the first example, a jurisdiction has deposited the instrument of ratification

FIGURE 9. **Date of deposit, entry into force and date of effect of the MAAC**

Example 1: deposit of the ratification instrument by 31 August in a given year.



Example 2: deposit of the ratification instrument after 31 August in a given year.



of the MAAC on 15 January 2018. Therefore, the MAAC entered into force for this jurisdiction on 1 May 2018 and came into effect for taxable periods starting on or after 1 January 2019. Assuming that the tax year coincides with the calendar year,[59] the first taxable period covered by the MAAC is 2019. In the second example, a jurisdiction deposited the instrument of ratification of the MAAC after 31 August 2018. Therefore, the MAAC entered into force at the beginning of 2019, meaning that it became effective for taxable periods starting on or after 1 January 2020.

Therefore, for a jurisdiction that has committed to commence automatic exchanges in a given year (Y) and assuming that its tax year is the calendar year, that jurisdiction will need to ensure it has signed and ratified the MAAC before 31 August of the year that is two years prior to the commencement year (Y-2). For example, to start exchanges in September 2022 with respect to the calendar year 2021, the MAAC should be in effect for that calendar year 2021 and therefore the ratification instrument of the MAAC should be deposited no later than 31 August 2020.[60]

However, where the jurisdiction has a tax year which diverges from the calendar year, the situation is different.

5.3.2. Diverging tax year

The majority of the jurisdictions implementing the Standard have a tax year that coincides with the calendar year (i.e. from 1 January to 31 December). However, some jurisdictions have a tax year that diverges from the calendar year. This is denominated as a diverging tax year and it can cover any 365-day period as defined by the jurisdiction. A typical example of a diverging tax year is from 1 April Y to 31 March Y+1.

The concept of a diverging tax year is relevant for the purposes of exchanging information under the Standard because it will determine the taxable period that is covered by the MAAC and therefore the first year under which exchanges are allowed to take place under the Standard. Indeed, the MAAC is effective with respect to a taxable period while the CRS MCAA is in effect for a full calendar year. In case of a diverging tax year, the first taxable period for which the MAAC will be in effect will not be a full calendar year. Therefore, the CRS MCAA will not be in effect for the full calendar year, which would postpone the first exchanges by one year.

Box 5 provides an example of a case where both jurisdictions have the calendar year as their tax year, and a case where one of the two jurisdictions has a diverging tax year and how it affects the respective dates of entry into effect of the MAAC and the CRS MCAA.

5.3.3. Declaration on the effective date for exchanges of information under the Multilateral Competent Authority Agreement on Automatic Exchange of Financial Account Information

To address the difficulties arising from date of effect of the MAAC, a unilateral declaration has been developed on the basis of Article 28(6) of the MAAC which allows Parties to mutually agree that the MAAC has effect for administrative assistance related to earlier taxable periods.

This declaration on the effective date for exchanges of information under the CRS MCAA would address the two situations mentioned above where the MAAC is not in effect for the calendar year for which the jurisdiction is committed to automatically exchange CRS data, including in the case of a diverging tax year (see Figure 9 and Box 5).

The unilateral declaration allows Parties to the MAAC to align the date of entry into effect of the CRS MCAA with the timeline provided in their notifications pursuant to Section 7(1)(a) on "Legislation and due diligence deadlines" (see Table 11). It also covers related follow-up exchanges of information on request. However, this acceleration the date of effect of the MAAC is only applicable between those Parties that have formulated the same unilateral declaration. So far, over 75 jurisdictions are covered by a unilateral declaration on the date of effect of the MAAC for exchanges under the CRS MCAA.

If a jurisdiction wishes to lodge this unilateral declaration, it has to contact the CB Secretariat (cb.mac@oecd.org) to initiate the process. The unilateral declaration shall be transmitted via diplomatic channels to the OECD or the CoE that would in turn notify all Parties to the MAAC.

59. With respect to jurisdictions with a tax year diverging from the calendar year, see Subsection 5.3.2 of the toolkit.

60. Unless a unilateral declaration allowing for an earlier date of effect is signed by the jurisdiction and other Parties (see Subsection 5.3.3 of the toolkit).

For example, if a jurisdiction intends to commence exchanges of information by September 2021 but deposits the instrument of ratification of the MAAC between 1 September 2019 and 31 December 2019, it will have to lodge a unilateral declaration to be able to exchange information in 2021 with those other jurisdictions that have also lodged the unilateral declarations.

Box 5. Consequence of the tax year on the date of effect of the CRS MCAA

Date of effect for two jurisdictions with a tax year aligned with the calendar year

In jurisdictions A and B, the tax year is the calendar year. Both jurisdictions signed the CRS MCAA in 2020 and they have provided all the required notifications in July 2020. Both jurisdictions also use the calendar year as the reporting period for CRS purposes.

Jurisdiction A signed the MAAC on 10 April 2020 and deposited its ratification instrument on 20 July 2020. The MAAC entered in force for jurisdiction A on 1 November and is effective for the tax period beginning on or after 1 January 2021.

Jurisdiction B signed the MAAC on 2 January 2019 and deposited its ratification instrument on 15 May 2019. The MAAC entered in force for jurisdiction B on 1 September 2019 and is effective for the tax period beginning on or after 1 January 2020.

The first CRS reporting period for which the CRS MCAA will be in effect between jurisdictions A and B is the reporting period beginning on 1 January 2021 as it is the first reporting period commencing on or after the latest date of entry into effect of the MAAC for both jurisdictions. This means that CRS exchanges between jurisdictions A and B relating to the calendar year 2021 will be allowed to take place by September 2022.

Date of effect where one jurisdiction has a diverging tax year

In jurisdiction C, the tax year is the calendar year, while in jurisdiction D the tax year is from 1 April to 31 March. Both jurisdictions signed the CRS MCAA in 2020 and they have provided all the required notifications in July 2020. They are both committed to start exchanges in 2022 with respect to the calendar year 2021.

Jurisdiction C signed the MAAC on 2 January 2019 and deposited its ratification instrument on 15 May 2019. The MAAC entered in force on 1 September 2019 and is effective for the tax period beginning on or after 1 January 2020.

Jurisdiction D signed the MAAC on 10 April 2020 and deposited its ratification instrument on 20 July 2020. The MAAC entered in force on 1 November 2020 and is effective for periods beginning on or after 1 January 2021. Since jurisdiction D has a diverging tax year, its tax year in 2021 starts on 1 April 2021. Therefore, while the MAAC is in effect for the taxable period starting on 1 April 2021, the first full calendar year covered by the MAAC is 2022.

Given that the CRS MCAA allows for exchanges of information related to a calendar year and requires legislation to be in place to allow for collection and reporting of information related to such calendar year, it will only allow for exchanges between jurisdictions C and D for the calendar year 2022. Therefore, the first exchanges would take place between the two jurisdictions by September 2023, unless they have formally agreed on an earlier effective date in order to allow exchanges to take place in September 2022 (see Subsection 5.3.3 of the toolkit).

6. Domestic legal framework

In addition to introducing an international legal framework to permit the exchange of information under the CRS-AEOI standard, jurisdictions must also put in place a domestic legal framework before exchanges can commence. The domestic legal framework:

- sets the due diligence and reporting requirements on Financial Institutions
- provides a legal basis within the jurisdiction to permit the automatic exchange of information
- introduces measures to ensure effective implementation.

The domestic legal framework typically requires the introduction of primary legislation, such as an act of parliament or legislative decree. In some jurisdictions, this legislation should only be introduced once the international legal framework to exchange information has been put in place, although it is preferable to decouple the two processes if possible. For jurisdictions which require domestic legislation to give effect to international treaties, such as the signing of the MAAC, the legislation can be adapted to also serve this purpose.

This part of the toolkit is set out in three sections which reflect the main steps in decision making for policymakers and government legal teams.

- The first section sets out the key issues to consider when structuring CRS legislation (step 1)
- The second section takes an issue by issue look at each element of the Standard intended to ensure effective implementation in practice, where the objective is clearly defined but where jurisdictions have discretion on the approach taken (step 2).
- The third section provides descriptions on the optional provisions of the CRS and detail to help policymakers determine whether such provisions may be appropriate for their jurisdictions (step 3).

As the legislative framework of each jurisdiction will be subject to assessment by peer review, these sections have noted some of the common pitfalls where approaches have been determined to be inconsistent with the ToR, as well as any other issues to look out for.

6.1. STEP 1: STRUCTURING THE LEGISLATIVE FRAMEWORK

The domestic legislation required to implement the Standard serves two key purposes:

- to impose obligations on certain persons in relation to the due diligence and reporting requirements
- to introduce measures which ensure effective implementation of the Standard.

The Standard does not prescribe the manner in which these rules are transposed and this will need to be tailored to the domestic legislative context of each jurisdiction. However, to ensure the Standard is fully implemented, the domestic framework to implement the due diligence and reporting rules on Financial Institutions **must be legally binding and must incorporate all of the required elements**.

When translating the Standard into a jurisdiction's legislative framework, policymakers will need to take two key structural decisions for drafting purposes:

- The first decision is whether the obligations on Financial Institutions under the CRS and its Commentary are made by reference to the Standard itself, or fully set out in domestic legislation (transposition of due diligence and reporting obligations).
- The second decision is the extent to which the legal basis to implement the Standard is made through primary legislation, secondary legislation or guidance.

6.1.1. Step 1A: How should a jurisdiction transpose the due diligence and reporting requirements: "copy out" or "reference" method?

The CRS has been drafted in a manner to make transposing the due diligence and reporting obligations on Financial Institutions (CRS, Sections I to VII) into domestic legislation as easy as possible.

- Section I of the CRS sets out the information that must be reported in respect of Reportable Accounts.
- Sections II to VII set out the due diligence that Financial Institutions must carry out to identify which Financial Accounts are Reportable Accounts.
- While Section VIII does not include requirements on Financial Institutions as such, but it includes defined terms which the other Sections rely on, including the definition of Financial Institution. Therefore these defined terms must also be fully transposed into domestic legislation.

Jurisdictions can transpose these obligations and definitions into domestic legislation by either:

- copying the full set of requirements of Sections I to VIII into legislative text (the "copy out" method)
- introducing a legislative requirement on Financial Institutions to refer to Sections I to VIII in the CRS, with a requirement to follow the obligations set out therein (the "reference" method).

The decision to use the "copy out" method as opposed to the "reference" method is one which may be limited by the legislative context. A jurisdiction may determine that obligations can only be imposed on persons where these obligations are fully set out in domestic legislation. It may also be the case that all obligations should be set out in the official language of the jurisdiction and as such reference to obligations in English or French may not be permissible, or not the preferred approach (see Box 6).

The Global Forum Secretariat has developed models of legislation based on the "copy out" and "reference" methods.

Comprehensive model legislation using the reference method is available in Annex C of the toolkit. This model has been developed to allow a jurisdiction to fully implement the CRS and its Commentary through a single legislative instrument.

Model legislation following the "copy out" approach is also available to competent authorities upon request (gftaxcooperation@oecd.org).

These models illustrate how the CRS and its Commentary can be introduced in the domestic legislation of the implementing jurisdiction. They offer full alignment with the requirements of the Standard, so as to mitigate the need for further amendments at a later date. However, jurisdictions may need to adapt them to their specific circumstances.

Box 6. **Language translation and domestic legislation**

Where jurisdictions do not have English or French as an official language and must ensure that all elements of their domestic legal framework are in their official languages, they should carefully consider how best to translate each term in a manner that ensures full consistency with the requirements of the Standard.

As the "copy out" method will involve full transposition of the CRS rules into domestic legislation, this translation exercise will be more extensive than where the "reference" method is taken. Nevertheless, even the "reference" method will typically require some terminology to be translated for inclusion in the domestic legislation. Furthermore, having translations of the requirements in CRS and its Commentary in guidance can be helpful to ensure compliance by Financial Institutions even where the legal basis refers to the official OECD versions.

Jurisdictions with official languages in common have often worked together to address the particular challenges of translation and have even set up working groups for this purpose. The domestic legislation of CRS participating jurisdictions which have already been translated can also be a helpful tool to legal drafters or legal translators in newly committed jurisdictions.

The Finnish experience

Finland's Constitution requires that any legislation including its interpretive guidance must always be made in its official languages which are Finnish and Swedish. When implementing the Standard, translating its defined terms posed a challenge, particularly where it included new terminology.

Finland first reviewed whether there were any existing terms in the official languages that would fit to this context. However, many existing terms had a different meaning and context, either in other Finnish legislation or in business practice. When translating, Finnish officials cooperated with its industry to introduce a number of new terms into domestic legislation, which in practice meant creating new Finnish and Swedish words. Where similar terms already existed, such as in its FATCA IGA, these were used as much as possible (although they were defined for the purposes of the CRS context).

While Finnish legislation used a reference method which requires that the CRS and its Commentary be used as a source of interpretation, Finland still had to make this available in its official languages. Finland has also made parts of the Implementation Handbook and all relevant FAQs available in Finnish and Swedish on the Finnish Tax Administration's website.

Source: Finnish Tax Administration.

Even where the model rules are adopted with minimal change, jurisdictions may still wish to create guidance to aide understanding by their Financial Institutions of their new obligations.

The Global Forum Secretariat remains available to assist implementing jurisdictions in the drafting of their CRS domestic legislation to ensure that it meets the Standard.

"Copy out" method

The "copy out" method is where jurisdictions incorporate the requirements of the CRS by copying and inserting the content of Sections I to VIII into its domestic legal framework, subject to certain adaptations.

There are different ways to "copy out" the CRS and its Commentary into the domestic legal framework. Taking into account the complexity and the extent of the provisions required to introduce the due diligence and reporting obligations, as well as the definitions, implementing jurisdictions should consider what provisions should be introduced in the primary legislation, the secondary legislation or another binding legal instrument.

It is advisable to introduce provisions in the primary legislation to cover the main obligations and to keep the detail of the due diligence, reporting requirements and definition for either:

- an annex or schedule of the primary legislation
- secondary legislation or another binding legal instrument.

This approach would facilitate the legislative process while ensuring the integrity of the due diligence procedure and definitions.

In any case, the CRS should be adapted to reflect the options taken by the jurisdictions as well as the relevant dates, the lists of Reportable Jurisdictions and Participating Jurisdictions, and the inclusion of any jurisdiction-specific lists of Excluded Accounts and Non-Reporting Financial Institutions.

Substantive additional detail

Some requirements under the CRS are included in the body of its Commentary and not set out in the text of the CRS itself. Jurisdictions must therefore be sure to also reflect all areas of interpretation and any substantive additional detail set out in the Commentary in the domestic legislative framework (see Annex B of the toolkit). This can be done by any of the following methods:

1. Introducing a requirement on Financial Institutions to interpret the rules in line with the Commentary (this is the approach set out in the model "copy out" rules). Such a requirement can be included in the primary or secondary legislation, or another binding legal instrument.
2. Incorporating each of the requirements of the substantive additional Commentary into legislation, in addition to the copied out rules. Depending on the method followed to copy out the CRS in the domestic legal framework, such detail can be added in either (i) the annex or schedule, or (ii) the secondary legislation or another binding legal instrument.
3. Incorporating the text of the Commentary into legally binding guidance.

These methods can also be introduced in combination with the requirement to interpret the rules in line with the Commentary acting as an effective reinforcement of the other possible options.

Table 12 presents some common pitfalls identified where the "copy out" method was followed.

"Reference" method

Fully translating the requirements of the CRS and its Commentary into domestic legislation under the "copy out" method requires significant legal drafting resources and has in practice often resulted in unintended gaps requiring a further round of legislative amendments. Recognising these challenges, many jurisdictions have adopted the "reference" method.

Table 12. **"Copy out" method – Common pitfalls**

Adapting rules to jurisdiction's circumstances	Certain jurisdictions have sought to adapt the requirements to reflect their particular circumstances. This has included adopting terminology which is already used in other legislation to refer to similar concepts, such as existing definitions of financial institution or account holder. This has frequently been determined to result in a divergence from the Standard, and as part of the assessments on the legal framework, recommendations to address any deficiency have been made.
Paraphrasing definitions and requirements	Similar to adapting the requirements to jurisdiction's circumstances, where jurisdictions have paraphrased the obligations, in order to follow existing legislative drafting style or to incorporate the rules into existing legislation, deficiencies in the requirements have often been identified.
Lost in translation	Jurisdictions which have to translate the definitions and requirements from English or French into the jurisdiction's official language will have to pay close attention to ensure that the intended CRS definitions and requirements remain unchanged.
Not reflecting the substantive additional detail in a binding instrument	Where the substantive additional detail has not been incorporated into the domestic legal framework through a binding instrument, it has usually resulted in deficiencies in the legal implementation of the Standard. For instance, some jurisdictions have not incorporated some or all of this detail or have only incorporated it in a non-binding instrument.

However, jurisdictions will have to consider whether such an approach is possible, taking into account its legal tradition.

Referencing the CRS and its Commentary in domestic legislation provides a number of benefits to the jurisdiction:

- It can act as a substantial safeguard to ensuring that the domestic legislation does not diverge from the Standard.
- This in turn greatly reduces the risk of having to amend legislation at later date to address deficiencies.
- Fully referencing the CRS and its Commentary can allow future developments in interpretation of the Standard to be automatically reflected in the legal framework.[61]
- It greatly facilitates the legislative process as the implementation of the Standard can be done with relatively few provisions.

The "reference" method model rules demonstrate how this works in practice. The model rules:

1. define the CRS as including its Commentary to ensure that the substantive additional detail is introduced in the domestic legal framework
2. introduce an obligation on Reporting Financial Institutions to carry out the due diligence obligations under Sections II to VII of the CRS
3. introduce an obligation on Reporting Financial Institutions to report the information set out in Section I of the CRS
4. require that Financial Institution be defined, and all other terms for the purposes of due diligence and reporting, in line with the definitions under Section VIII of the CRS.

The remainder of the model rules then set out the jurisdiction specific options which are covered under Sections 6.2 and 6.3 of this toolkit.

Some jurisdictions have extended their reference method to also refer to the OECD's list of FAQs on the application of the CRS in their legislative framework at the same time as referencing the Commentary. The answers to such questions provide further precision on the CRS and help to ensure consistency in implementation. While it is expected that most jurisdictions would readily be able to apply the conclusions found in the FAQs, it is not a requirement to legislatively reference the FAQs providing no issues arise in the jurisdiction in the application of the subjects covered. Two FAQs that jurisdictions should pay particular attention to when considering their legislative framework are in respect of Section II-VII of the CRS: FAQ 22 on strong measures to obtain self-certifications (see Subsection 6.2.8 of the toolkit) and FAQ 26 on Controlling Persons (see Box 8).

A summary of the key differences between the "copy out" and "reference" methods is included in Figure 10.

61. Some jurisdictions have also fully referenced the CRS and its Commentary as it was put in place and agreed at a certain point in time. This has allowed them to incorporate many of the advantages of the reference method but does not introduce an ambulatory approach of interpretation. In such cases, the legislative framework may at a later stage have to be revised to reflect any developments.

FIGURE 10. **Comparison of the "copy out" and "reference" methods**

6.1.2. Step 1B: How should the legal framework be structured across primary and secondary legislation, and guidance?

The majority of jurisdictions have implemented their legislative framework via a combination of primary and secondary legislation. This multi-layered approach can give jurisdictions the flexibility to update their legislative framework without always requiring their legislative assemblies to pass primary legislation in every instance.

Flexibility to adapt the legislative framework can be helpful to jurisdictions that need to carry out the following:

- periodic updating of the list of Reportable Jurisdictions following activation of new exchange relationships entered into
- introduction of any amendments to address any deficiencies identified by the jurisdiction following implementation and/or following Global Forum assessment
- incorporation of any future developments of the CRS or clarifications of its interpretation (CRS Commentary, FAQs).

In order to benefit from such flexibility, jurisdictions have often implemented as many of the CRS requirements as possible in the legislative format that is most easily amended while still remaining binding in law. For many jurisdictions, this has meant including the due diligence and reporting requirements in secondary legislation, taking the form of regulations issued by way of delegated authority (to a minister or statutory body), and in some cases via binding guidance.

Table 13. **Possible content of binding and non-binding guidance**

What can non-binding guidance include?	What can binding guidance include?

• Information complementary to the binding legislation
  ◦ to make the rules more easily understood
  ◦ to contextualise or demonstrate the application of the rules in the jurisdiction, e.g. how the CRS definitions could apply to certain entities
• Details on how to report, including:
  ◦ an explanation of CRS XML Schema requirements (including translations of the descriptions where the language of the jurisdiction is not English or French)
  ◦ details on how to submit reports through the jurisdiction's AEOI portal
• Publicly available information on the jurisdiction's administrative compliance framework, including:
  ◦ guidelines to set out what Financial Institutions can expect during verification activities (such as an audit)
  ◦ details on the application of penalties and the appeal rights of persons that are subject to a penalty
• Information to the general public in respect of their responsibilities as Account Holders in providing their Financial Institutions with self-certifications.
	• All information that can be included in non-binding guidance
	• Detail on obligations not covered elsewhere in the legislative framework but which are still requirements for the implementation of the Standard, namely:
	  ◦ substantive additional detail outlined in the Commentary[62]
	  ◦ jurisdiction-specific lists of Non-Reporting Financial Institutions and Excluded Accounts
	  ◦ lists of Participating Jurisdictions and Reportable Jurisdictions.

62. This can be done by incorporating the relevant parts or the full CRS Commentary, translated into the jurisdiction's language where necessary. See also Annex B of the toolkit.

The model rules based on the "copy-out" approach are composed of primary and secondary legislation. In both cases, the technical requirements for the implementation of the Standard (e.g. technical modalities of reporting by Financial Institutions such as the schema format and AEOI portal to be used) can be detailed in guidance.

Guidance

Many jurisdictions have issued guidance as part of their communications and outreach strategies to assist Reporting Financial Institutions in complying with their obligations. Guidance offers the benefit of allowing the requirements, set out in primary or secondary legislation, to be more easily understood and contextualised with jurisdiction specific examples to aide application of the rules.

The Standard requires jurisdictions to implement all of the substantive definitions, due diligence and reporting obligations into their legislative framework in a manner that is binding. Therefore, the content of a jurisdiction's guidance will vary depending on whether the guidance is binding or not binding in nature, and what provisions have been included in their legislation (see Table 13).

Table 14 describes some common pitfalls identified in the peer review process.

Table 14. **Guidance – Common pitfalls**

Implementing substantive additional detail of the Commentary in non-binding guidance	In order to ensure that the Standard is implemented in full, the substantive additional detail must be included in the domestic legislative framework, and it must be binding (see Annex B of the toolkit). Issues in implementation have arisen where jurisdictions have omitted this detail from their primary or secondary legislation. This has typically been the case where jurisdictions have adopted the "copy out" method, and only included the body of the CRS into their legislation with no binding requirement that it must be interpreted in line with the Commentary. Where jurisdictions are unable to issue binding guidance to cover the missing substantive additional detail, its inclusion in non-binding guidance raises concerns for the effectiveness of the jurisdiction's legislative framework.
Applying the CRS requirements in a jurisdiction-specific context that is not in line with the Standard	While guidance can give helpful clarity on the application of the CRS within a jurisdiction, caution should be made where the reporting status and obligations of Entities in a jurisdiction is pre-determined. It might be clear in certain cases that an Entity in a jurisdiction falls within a particular CRS definition, for example, the jurisdiction's Central Bank. In contrast, for many other Entities in a jurisdiction that may be defined by characteristics prescribed in other legislation, pre-determining the CRS status based on that other legislation can result in classifications that are not in line with the Standard. For example, a jurisdiction may decide that all domestically regulated investment funds is synonymous with the definition of Investment Entity under the CRS and link these definitions. While in practice such funds can meet the definition, if this approach excludes the possibility of other entities, such as non-regulated entities, from meeting the definition of Investment Entity, this has been considered a deficiency.
Guidance which conflicts with the CRS requirements introduced in legislation and creates deficiencies	More generally, jurisdictions should always ensure that the guidance, whether binding or non-binding, does not contradict the requirements of the Standard. Even non-binding guidance which departs from the primary or secondary legislation could be relied on by Financial Institutions and for this reason, such discrepancies have been considered as a deficiency.

Summary of common approaches

The model rules based on the "reference" method implement all CRS requirements in primary legislation. Nevertheless, guidance may be required to define the technical reporting requirements for Financial Institutions and provide additional information to assist them in the implementation of their CRS obligations.

The "copy out" model rules implement the Standard through primary and secondary legislation.

In any case, jurisdictions will have to consider their own legislative context and processes when determining how to implement the requirements of the Standard. Table 15 outlines the approaches often taken by jurisdictions in this process.

Table 15. **Common structuring of the CRS legislative framework**

Key CRS elements	Primary legislation	Secondary legislation	Binding guidance	Non-binding guidance
Definitions	Definitions relevant for the primary legislation (for example, the Agreement, the competent authority, the CRS)	Further definitions (those not required in the primary legislation)		
Obligation to conduct due diligence, keep records and report information	Main obligations (for example, filing an Information Return, conducting due diligence)	Detailed due diligence (including due diligence deadlines) Substantive additional detail Optional provisions Reporting details and Date List of Excluded Accounts and Non-Reporting Financial Institutions List of Participating Jurisdictions and Reportable Jurisdictions		
Technical reporting requirements			Manner of reporting (in line with XML schema, via specified portal)	
Powers to issue subsequent legal instruments	Powers to introduce secondary legislation /guidance	Powers to introduce guidance		
Penalties	Penalties (on Reporting Financial Institutions and on Account Holders and Controlling Persons			
Primacy of CRS legislation	Provision to ensure that the CRS legislation prevails over any other legislation to the contrary			
Confidentiality	Confidentiality provision			
Anti-avoidance	Anti-avoidance provision	Additional guidance		Examples of cases where the measure should be applied

6.1.3. Step 1C: Can a jurisdiction rely on existing domestic legislation?

When structuring CRS legislation, jurisdictions may make a policy choice to adapt or make use of existing legislation. This is commonly done by either inserting specific CRS legislative provisions into consolidated tax legislation (tax codes), or by adapting or cross referencing existing legislation to incorporate the CRS requirements.

Incorporating CRS requirements into consolidated tax codes

When incorporating CRS legislative provisions within existing tax legislation (tax law or code), jurisdictions should always ensure that this tax legislation does not limit the scope or extent of the CRS requirements.

What to look out for

- Tax legislation (tax law or code) may be limited in its scope to particular persons or entities within the jurisdiction and therefore may not cover all those covered by the CRS. Indeed, CRS requirements should extend to all concerned persons, not only to persons that are tax resident in the jurisdiction or liable to tax by other means. Certain CRS provisions apply to non-resident persons, including Account Holders and branches of foreign Financial Institutions who might not be subject to CRS obligations in their jurisdiction of incorporation.
- The definitions otherwise applicable in the tax legislation may not be in line with the CRS definitions for the same terms. It is critical for the full implementation of the Standard that the CRS definitions apply independently of any other conflicting definitions. To prevent cross over in interpretation of any existing definitions used in the tax legislation (or any other domestic laws) with CRS definitions, jurisdictions can clearly specify that only CRS definitions are application for CRS purposes (and vice versa).

Adapting FATCA legislation to meet CRS requirements

Many jurisdictions which now commit to implementing the Standard already have legislation in place requiring Financial Institutions to carry out due diligence and reporting obligations to comply with FATCA agreements. While the CRS was designed to build on obligations contained within FATCA Model I Intergovernmental Agreements (IGA), there are a number of substantial differences where the legislation will have to be adapted to be in line with the Standard.

For these reasons, it can be challenging to adapt existing FATCA legislation to introduce CRS due diligence and reporting obligations. Jurisdictions that decide to consolidate FATCA and CRS legislation should be conscious of these distinctions (see Box 7 for an example). This is not the approach followed in the model rules.

What to look out for

- The distinctions between FATCA and the CRS, which include differences in:
  - key definitions
  - the due diligence obligations on Financial Institutions
  - the characteristics of reportable persons: the CRS concerns the identification of tax residents whereas FATCA considers citizenship and permanent residents ("US Persons" definition).
- Due diligence undertaken for FATCA purposes cannot be relied upon because of the distinctions in the definitions and requirements. Therefore CRS provisions will have to introduce a new obligation on Financial Institutions to carry out due diligence, including on Preexisting Accounts which may already have been subject to due diligence for FATCA purposes.
- The CRS has more limited definitions of Non-Reporting Financial Institutions and Excluded Accounts:
  - Jurisdictions will not be able to reference the same Non-Reporting Financial Institutions and Excluded Accounts for CRS purposes, and will have to undergo the Global Forum's Non-Reporting Financial Institutions and Excluded Accounts assessment process for any jurisdiction-specific exclusions.
  - The CRS provisions will often impose obligations on Financial Institutions that might previously have been exempt.

A detailed list of the distinctions between the CRS and FATCA can be found in Part III of the Implementation Handbook.[63]

63. See the OECD (2018), *Standard for Automatic Exchange of Financial Information in Tax Matters - Implementation Handbook*, op.cit.

Relying on existing AML/CFT legislation for the definition of Controlling Person

Recognising that Entities are not necessarily tax resident in the same jurisdiction as the beneficial owners of that Entity, the CRS includes a requirement to report information on Financial Accounts held by Entities to both (i) any foreign jurisdiction(s) where the Entity is a tax resident and (ii) any foreign jurisdiction(s) where the beneficial owners of the Entity are tax resident(s).

To this end, the CRS includes a requirement to carry out due diligence and reporting in respect of "Controlling Persons"; a term which corresponds to the definition of beneficial ownership as described in the FATF 2012 Recommendation 10 and its Interpretive Note.[64] This coherence in definitions is intended to ensure consistency with the customer due diligence steps that Financial Institutions would otherwise be undertaking for AML/CFT purposes. Box 8 provides additional guidance regarding the term "Controlling Person".

However, when jurisdictions rely on AML/CFT legislation that is not in line with these Recommendations, for the purposes of determining Controlling Persons, this leads to a deficiency in their domestic legal framework to implement the Standard. Table 16 illustrates some common pitfalls identified in the peer review process.

Jurisdictions can ensure the definition of Controlling Person in their domestic legal framework is in line with the Standard by either:

- **Using the reference method:** Where jurisdictions have fully adopted a reference method and have required that the obligations and definitions must be interpreted in line with the CRS Commentary, the substantive requirements for the definition of Controlling Person will be met. Even where jurisdictions have updated their AML/CFT legislation in line with the FATF recommendations, the reference method can provide jurisdictions with an extra layer of comfort.
- **Incorporating the relevant CRS definition and the Commentary on the definition of Controlling Person into the domestic legal framework:** Where jurisdictions have adopted the "copy out" method, they will need to ensure that all components of this definition described in the Commentary are incorporated to ensure correct interpretation.

Box 7. **The United Kingdom's approach**

The United Kingdom (UK) has put in place consolidated FATCA and CRS legislation. However, the UK has adopted the reference method for both sets of obligations which prevents conflict between the requirements: the UK's legislation makes direct reference to both (i) the CRS and (ii) the UK-US FATCA IGA.

This approach has been applied for both the definitions and the due diligence and reporting obligations.

Example of reference method to definition in UK legislation:

> *2. (1) In these Regulations, a "reportable account" means—*
>
> *(a) an account which is a reportable account within the meaning of the relevant agreement,*

Example of reference method to due diligence in UK legislation:

> *3. (3) The due diligence procedures are—*
>
> *[…]*
>
> *(b) in relation to a reporting financial institution under the CRS, set out in Sections II to VII of the CRS,*
>
> *(c) in relation to a reporting financial institution under the FATCA agreement, set out in Annex I to that agreement.*

Source: The International Tax Compliance Regulations 2015 (as amended) available at: https://www.legislation.gov.uk/uksi/2015/878/contents.

64. For Entity Accounts, a Reporting Financial Institution may rely on information collected and maintained pursuant to the Reporting Financial Institution's AML/KYC Procedures to determine the Controlling Persons. For New Entity Accounts this is only possible where the AML/KYC Procedures are in line with FATF 2012 Recommendations. In practice, this may mean that for Preexisting Entity Accounts, the Controlling Persons identified may however be determined on the basis of previous AML/KYC definitions of beneficial owners, until such a time when the Reporting Financial Institution is required to update its AML/KYC information on its Account Holders.

- **Relying on existing (FATF 2012 compliant) AML/CFT legislation:** In such instances, the definition of "Controlling Person" in the legislation could be stated as equivalent to the definition of beneficial owner and specify the AML/CFT legislation where this definition can be drawn from (see also Boxes 8 and 9).

Where the reference method has not been adopted, the jurisdiction should also ensure that the requirement of paragraph 137 of the Commentary in respect of reliance on AML/KYC procedures has also been incorporated into the legal framework.

What to look out for

Irrespective of the approach taken, the jurisdiction should undertake a comprehensive analysis of the definition of beneficial owner in its AML/CFT legislation and the methodology required to be applied by Financial Institutions to identify them. If a jurisdiction decides to rely on its existing AML/CFT legislation, such analysis should be especially exhaustive to ensure that it is fully in line with the Recommendations 10 and 25 and their Interpretive Notes as adopted by the FATF in 2012 because any discrepancy can result in a significant

Box 8. **Understanding the "Controlling Person" definition**

The definition of Controlling Person of the CRS-AEOI standard is spread across three sources: the CRS, its Commentary and the FATF Recommendations.

Section VIII.D.6. of the CRS sets out the definition of Controlling Person:

> *The term "Controlling Persons" means the natural persons who exercise control over an Entity. In the case of a trust, such term 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, and in the case of a legal arrangement other than a trust, such term means persons in equivalent or similar positions. The term "Controlling Persons" must be interpreted in a manner consistent with the Financial Action Task Force Recommendations.*

As with all elements of the CRS, the paragraph is to be interpreted in line with the accompanying Commentary. It is notable that there is also a clear requirement to interpret the definition in a manner consistent with the FATF Recommendations.

The Commentary on Section VIII.D.6, set out in paragraphs 132 to 137, gives substantive further detail on the definition of Controlling Persons. It clarifies that the term "Controlling Persons" corresponds to the term "beneficial owner" as described in Recommendation 10 and the Interpretive Note on Recommendation 10 of the FATF Recommendations as adopted in February 2012.

This is further elaborated with specific detail on the Controlling Persons of Entities that are legal persons (paragraph 133), trusts (paragraph 134), legal arrangements other than a trust (paragraph 135), and legal persons that are functionally similar to trusts (paragraph 136).

Paragraph 137 is not directly concerned with the definition of Controlling Person itself but rather with the procedures taken by Reporting Financial Institutions to determine Controlling Persons. It sets out the basis on which Reporting Financial Institutions may rely on information collected pursuant to AML/KYC purposes to determine Controlling Persons. This paragraph therefore acts as a backstop to ensure that, should the existing AML/CFT legislation not align with the 2012 FATF Recommendations, Reporting Financial Institutions will be unable to rely on these procedures to determine Controlling Persons. For New Entity Accounts, these AML/KYC Procedures must always be consistent with Recommendations 10 and 25 of the 2012 Recommendations.

The 2012 FATF Recommendations 10 and 25 and their Interpretive Notes referred to in both the CRS and its Commentary are therefore key documents with respect to defining and applying the definition of Controlling Persons.

deficiency in the legal framework for CRS-AEOI. If there has been a recent FATF Mutual Evaluation Report, it may be useful to refer to the findings in that report so far as these are relevant to the meaning of beneficial owner and the findings remain current.

Relying on existing penalties legislation

Jurisdictions committing to implement the Standard will typically already have penalty frameworks in place concerning non-compliance with tax legislation and/or with AML/CFT legislation.

As the nature of the due diligence and reporting obligations are varied, and do not only concern the persons and duties covered by tax and AML/CFT frameworks, most jurisdictions have had to introduce new penalty provisions or amendments to existing ones in order to be able to sanction non-compliance with the CRS obligations.

The specific considerations on introducing penalties to address non-compliance, including when relying on existing penalties legislation, is addressed under Subsection 6.3.5 of the toolkit.

6.2. STEP 2: WHAT OTHER MEASURES ARE NEEDED TO ENSURE EFFECTIVE IMPLEMENTATION OF THE STANDARD?

The due diligence, reporting requirements, and associated definitions (CRS, Sections I to VIII) of the Standard are clearly specified and must be implemented consistently across all committed jurisdictions. However, there remain some elements of the Standard where the overall objective is set out, but each jurisdiction has discretion on the measures taken to meet that objective.

This includes measures under Section IX of the CRS to ensure effective implementation, such as to enable the relevant authority to verify Financial Institution compliance with the CRS requirements. It also includes certain other key decisions that jurisdictions have to make when implementing legislation, such as in respect of dates and filing to ensure proper functioning of the requirements.

Each jurisdiction will therefore have to introduce legislative provisions (or adapt the model rules) in respect of the following:

- dates for commencement and completion of due diligence requirements
- the date and manner of domestic filing by Financial Institutions
- a requirement on Financial Institutions to maintain documentation and records
- access and information gathering powers
- an appropriate penalty or sanctions regime
- measures to address circumvention of the requirements
- provisions to override any existing secrecy provisions (if needed)
- strong measures to ensure self-certifications are always obtained.

Box 9. **FAQ 26: Threshold for determining Controlling Persons of Entity**

Paragraph 133 of the Commentary on Section VIII provides an example threshold of 25%, with the expectation that each jurisdiction will explicitly specify the threshold in its CRS legal framework. Since 25% is only an example, the reference approach to incorporate the requirements set out in the Commentary is insufficient to legally incorporate this as the relevant threshold in the legal framework.

FAQ 26 clarifies that the appropriate threshold for determining a Controlling Person for CRS purposes cannot be higher than the threshold used for AML/KYC purposes. For example, if the AML/KYC threshold is 10%, the CRS threshold must also be 10% (or lower).

A jurisdiction may specify the percentage for the purposes of the threshold in the CRS legal framework. Alternatively it could cross reference the threshold used for AML/KYC purposes, an approach that has the advantage of not requiring an amendment of the CRS legislation in the event of change to the AML/KYC threshold in the future.

Source: CRS FAQs, Section II to VII, FAQ 26.

Table 16. **Relying on the AML/CFT legislation – Common pitfalls**

Compliance of the AML/CFT legislation definition of beneficial owner with the CRS definition of Controlling Person	Where existing AML/CFT legislation has been relied upon for determining Controlling Persons and it is not consistent with paragraphs 132 to 136 of the Commentary on Section VIII of the CRS, then this results in a deficiency in the implementation of the Standard. Comprehensive analysis of the AML/CFT legislation is therefore an important step before drafting CRS legislation if that legislation will rely on the definition of beneficial owner through cross reference.
Controlling Persons of trusts	Where the definition of beneficial owner of trusts does not identify all Controlling Persons of trusts, particularly "settlors" or "any other natural persons exercising ultimate effective control over the trust" then this results in a deficiency in the implementation of the Standard.
Controlling Persons of legal arrangements	Where the definition of beneficial owner does not identify all Controlling Persons of legal arrangements, including persons in positions similar to Controlling Persons of a trust, then this results in a deficiency in the implementation of the Standard.
Controlling Persons of legal persons	Where the existing AML/CFT legislation is relied upon and the threshold to identify the Controlling Persons for the purposes of legal persons has not been specifically referenced in the CRS legislation, the jurisdiction may receive a note to monitor that Financial Institutions apply the correct threshold in practice.
Higher threshold for control for CRS purposes than for AML/CFT purposes	Where the introduction of an ownership threshold for the purposes of Controlling Person is higher than required for AML/CFT purposes, this results in a deficiency. The requirement to have the same (or a lower) threshold for CRS purposes is explained under FAQ 26 (see Box 9).

6.2.1. Dates of due diligence requirements

A key decision when introducing the CRS legislation is determining the dates by which Reporting Financial Institutions will be required to fulfil their due diligence obligations. When deciding these dates, there are typically three key factors which must be considered:

1. when the draft legislation introducing the obligations on Reporting Financial Institutions will become law (and take effect)
2. how much time the jurisdiction wishes to give Reporting Financial Institutions to fulfil the due diligence obligations on Preexisting Accounts
3. the year in which the first exchanges will be carried out.

When the legislation takes effect

Reporting Financial Institutions will only be legally obliged to carry out due diligence once the relevant legislation is in place and has effect. The date selected to determine Preexisting Accounts (and distinguish them from New Accounts) should therefore be on or after the date of effect to ensure that all New Accounts are subject to the necessary due diligence procedures, i.e. that valid self-certifications are always obtained for New Accounts.

Jurisdictions should take into consideration the time needed by Financial Institutions to implement the due diligence procedures (e.g. training of employees, implementation of new on-boarding procedures for new clients and internal CRS compliance framework, adaptation of their IT systems). Sufficient time should therefore be provided between the passing of the CRS-AEOI legislation, its entry into force and date of effect, and the date for the commencement of due diligence obligations (where different from the date of effect). It is usually appropriate to provide at least a six-month period.

If a jurisdiction's legislative adoption process would envisage a CRS bill becoming law in June 2021 with immediate effect, then due diligence requirements could commence any time after this point. However, to ensure that Financial Institutions have sufficient notice, and to ensure synchronicity with subsequent reporting dates, the date chosen to define New Accounts and commence due diligence on them would usually be the start of a calendar year. Therefore, the legislation would define New Accounts as all accounts open on or after 1 January 2022 and the first year in which exchanges take place will be 2023.

Time needed for Preexisting Account due diligence

The Commentary to Sections III and V for Preexisting Individual Accounts and Preexisting Entity Accounts respectively set out the following expectations on jurisdictions for due diligence dates. The example dates hereafter are given in relation to the date the jurisdiction has selected to define Preexisting Accounts (all accounts opened and maintained on or before 31 December of the given year Z).

- Due diligence on Preexisting Individual Accounts that are High Value Accounts is expected to be completed by the end of the first year following the date selected to define Preexisting Accounts (31 December Z+1).
- Due diligence on Preexisting Individual Accounts that are Lower Value Accounts is expected to be completed by the end of the second year following the date selected to define Preexisting Accounts (31 December Z+2).
- Due diligence on Preexisting Entity Accounts is expected to be completed by the end of the second year following the date selected to define Preexisting Accounts (31 December Z+2).

While most jurisdictions have chosen to adopt the one year (for High Value) and two year (for all other Preexisting Accounts) approach, this is optional and jurisdictions may instead set out a shorter period providing it leaves sufficient time for their Financial Institutions to effectively carry out the necessary due diligence. Consultation with stakeholders, including

Table 17. **Example of due diligence and reporting date**

A jurisdiction is committed to start its first exchanges under the Standard in September 2024. The dates for carrying out due diligence and reporting the information are as follows (note that even when there is a later deadline to complete the due diligence with respect to Preexisting Accounts, they are reportable as soon as they are identified as such):

<table>
<tr><th>Accounts</th><th>Defined as</th><th colspan="4">Completion of due diligence and date of first exchange</th></tr>
<tr><td rowspan="2">New Accounts</td><td rowspan="2">A Financial Account maintained by a Reporting Financial Institution opened on or after 1 January 2023.</td><td>Completion of the due diligence as New Accounts are opened</td><td colspan="3">Ongoing from 1 January 2023</td></tr>
<tr><td>Date of first exchange of information by</td><td colspan="3">September 2024</td></tr>
<tr><td rowspan="3">Preexisting Accounts</td><td rowspan="3">A Financial Account maintained by a Reporting Financial Institution as of 31 December 2022.</td><td rowspan="2">Completion of the due diligence by</td><td>Individual High-Value Accounts</td><td>Individual Lower Value Accounts</td><td>Entity Accounts</td></tr>
<tr><td>31 December 2023</td><td>31 December 2024</td><td>31 December 2024</td></tr>
<tr><td>Date of first exchange of information by</td><td>September 2024</td><td>September 2024 or September 2025, depending on when identified as reportable.</td><td>September 2024 or September 2025, depending on when identified as reportable.</td></tr>
</table>

to understand the scale of their Preexisting Accounts and the ease with which the CRS due diligence can be carried out, can be helpful when determining these dates. In any case, once a Reportable Account is identified pursuant to the due diligence procedure it must be reported the following year. Table 17 provides a concrete example.

Year of first exchanges

Because of the time needed by Financial Institutions to carry out the CRS due diligence and identify Reportable Accounts, jurisdictions should factor in one full calendar year from the date when the CRS legislation takes effect before Reporting Financial Institutions begin reporting information and exchanges can commence.

Where jurisdictions have allowed their Reporting Financial Institutions up to two calendar years to fulfil the due diligence requirements in respect of Preexisting Individual Lower Value Accounts and Preexisting Entity Accounts, the jurisdiction will still be able to commence exchanges in the second year of due diligence (Z+2). The information that will be reported in this first year of exchange will include all Preexisting Individual Accounts that are High Value Accounts, as well as New Accounts (Individual and Entity). This first year of exchange will also include any Preexisting Individual Accounts that are Lower Value Accounts identified as Reportable Accounts in the first year of due diligence (Z+1). As all Preexisting due diligence should be completed in Z+2, the second year of exchange (Z+3) often results in a significantly greater number of Reportable Accounts being sent to exchange partners.

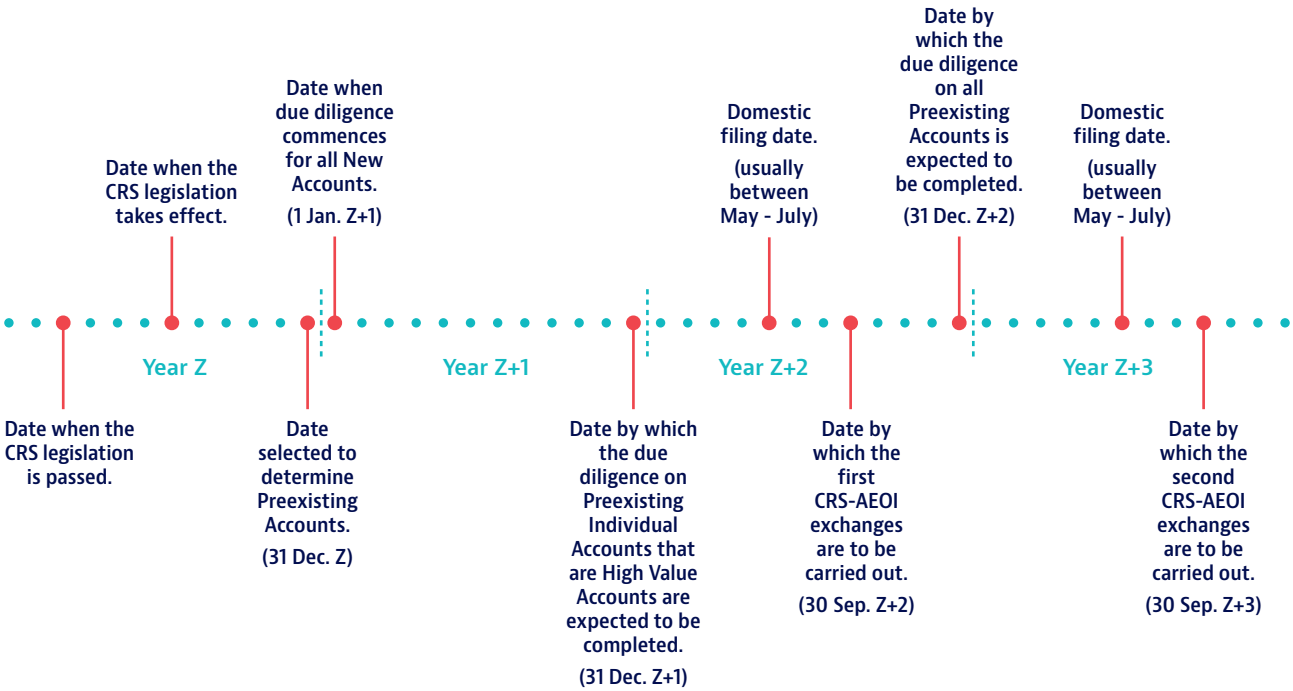
Figure 11 provides an example of due diligence and reporting timeline.

6.2.2. Filing requirements

What is required?

The Standard sets out the requirements on Financial Institutions to report the necessary information to their competent authority, and the requirements on the competent authority to send the information to its exchange partners within nine months from the end of the year (Z) to which the information relates (i.e. by 30 September Z+1). For this to work in practice, jurisdictions must ensure their legislative framework sets out a requirement on Financial Institutions to report, or "file", this information in advance of the exchanges taking place.

FIGURE 11. **Example of due diligence and reporting timeline**



Why is it important?

At a minimum, to enable competent authorities to meet the exchange deadline set out under the Standard, a jurisdiction's domestic legislative framework must set out an obligation on Financial Institutions to report the required information to the nominated authority, by a certain date.

In the absence of such a clear obligation, competent authorities would be unable to penalise Financial Institutions for failing to submit the required CRS data.

How can the requirement be implemented?

The legislative requirement to file the information must ensure that all required information under Section I of the CRS is reported by a specified date. The legislation may also set out the manner in which the information must be submitted, such as by way of an electronic "return".

Filing deadline

The date a jurisdiction chooses to require its Reporting Financial Institutions to submit a CRS return domestically is inherently linked to the requirement on jurisdictions to exchange the information with partners annually (i.e. by 30 September Y+1).

Jurisdictions reporting information in respect of a calendar year (Y) therefore have flexibility in choosing a date within the range of 1 January Y+1 to 30 September Y+1.

However, when determining the date, the jurisdiction will need to balance (i) the time needed by Reporting Financial Institutions to fulfil their reporting obligations and (ii) the time needed by tax authorities to prepare and exchange the information to partners once it has been received from Reporting Financial Institutions:

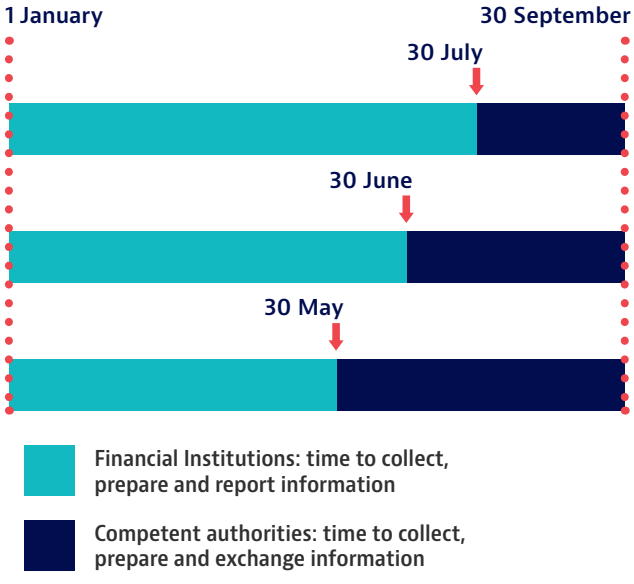
i. Financial Institutions will typically need time following the 31 December to:

   - collect all the required information in respect of the most recent reporting year from its internal systems and records. This includes identifying the relevant balances on the 31 December, and income reported to the Financial Accounts in the year to 31 December, in respect of their Reportable Accounts
   - ensure that the data to be reported is in line with the reporting requirements of the competent authority (such as the XML Schema requirements or any other format permitted domestically)
   - carry out any quality assurance checks such as sampling to ensure that the information to be reported is complete and accurate
   - submit any corrected files if issues have been identified on initial transmission, including if the information does not meet the required format (such as the XML schema requirements).

ii. Competent authorities will typically need time following submission of the Financial Institutions' returns and prior to the 30 September exchange deadline to:

   - identify and follow up with late filing Financial Institutions
   - prepare and validate the information for exchange, including sorting the information and carrying out any manual quality assurance checks on the information (see Subsection 7.2.3 of the toolkit)
   - transmit the information to exchange partners (See Subsection 7.2.4 of the toolkit).

FIGURE 12. **Commonly selected filing deadlines: balancing time needed by Financial Institutions and the competent authority**



Jurisdictions have typically opted for the filing deadlines of either 31 May, 30 June or 31 July in order to balance the time needed by both Financial Institutions and the competent authority. Consideration may also be taken of other reporting obligations on Financial Institutions, such as any FATCA or domestic tax reporting deadlines, other competing demands on the resource of the tax authority, or of public holidays (recognising that filing deadlines on Financial Institutions will also result in an increase in queries to the tax authority).

Manner of reporting

It will depend on each jurisdiction's practices whether legislation is needed to set out the manner of reporting and in many cases it will be possible to do this by way of issuing secondary legislation or guidance.

Jurisdictions which do require the manner of reporting to be set out in legislation will have to coordinate with the teams responsible for putting in place an AEOI portal or similar system to ensure that the legislation is aligned with the reporting tools they plan to develop (see Subsection 7.2.1 of the toolkit).

6.2.3. Record-keeping requirements

What is required?

Under the Standard, jurisdictions must have rules in place requiring Reporting Financial Institutions to keep records of the steps undertaken and any evidence relied upon for the performance of the due diligence and reporting procedures. The Standard also specifies that such records must be available for a period of not less than five years after the end of the period within which the Reporting Financial Institution must report the information.

Why is it important?

The record-keeping requirements on Financial Institutions are a vital component of a jurisdiction's administrative compliance framework. They allow a jurisdiction's supervisory authority to verify compliance with the due diligence and reporting requirements, including to ensure that all Reportable Accounts were identified and that the information reported in respect of these is correct. Moreover, having these records available can assist the tax authority in responding to any follow-up queries from those exchange partners that received the information. Follow-up may be necessary on behalf of an exchange partner to verify the accuracy of the information, whether due diligence was done correctly, or to obtain more information about the account or the Reportable Persons related to the account.

Box 10. **Example to illustrate record-keeping requirement**

A common deadline for the reporting of the information that has been used by jurisdictions is 31 May. For such jurisdictions, records should be kept for five years starting on 31 May of the year in which the information was reported to the tax authority. As due diligence is carried out in the year(s) prior to the year of reporting, in practice records are always required to be kept for longer than five years after they were collected or created for due diligence purposes.

If a Reporting Financial Institution carried out due diligence in 2020 on an account and identified it as a Reportable Account, and the reporting deadline is 31 May, this account will be reported for the first time by 31 May 2021. The Reporting Financial Institution should keep the relevant records in respect of their 2021 filing until at least 31 May 2026.

The timeframe continues to be extended so long as the account remains open in subsequent reporting periods. If the account remains open until the calendar year 2030, the relevant records will need to be retained until 31 May 2036, which is five years after the end of the last period in which information is reported in respect of those records (i.e. 31 May 2031).

The requirement to keep records related to the account for this period of time is not dependent on whether the account was identified as reportable. Therefore, in this example, even where the account has not been identified as a Reportable Account (i.e. 2020-35), the relevant documentation obtained and records of the steps undertaken must still be maintained until 31 May 2036.

How can the requirement be implemented?

Jurisdictions must require their Reporting Financial Institutions to maintain both:

- **records of any documentation obtained** in the performance of due diligence and reporting, e.g. a self-certification when a New Account is opened
- records of the **steps undertaken** for the performance of such procedures, e.g. how it performed the electronic record search for the Lower Value Preexisting Individual Accounts.

Furthermore, records must be kept for five years after the end of the period within which the Reporting Financial Institution must report the information (see Box 10).

Table 18 summarises some common pitfalls identified in the peer review process.

Table 18. **Record-keeping obligations – Common pitfalls**

Relying on record-keeping obligations under a pre-existing legal framework	When jurisdictions relied on record-keeping obligations introduced under the AML/CFT framework or under another pre-existing legal framework, deficiencies have often been identified as not all Financial Institutions, nor all records required to be kept, are covered by those frameworks (e.g. self-certifications). This is typically because pre-existing frameworks require the retention of records in relation to specific purposes (e.g. due diligence for AML/CFT purposes) and therefore do not extend to all aspects of CRS due diligence. Furthermore, the retention periods of such frameworks are often not aligned with the CRS requirements.
Failure to require records to be kept of both the steps undertaken and of the evidence relied upon	Deficiencies have been identified were the legislative framework has only required the retention of either the records of the steps undertaken or of the evidence relied upon for the performance of the due diligence and reporting requirements. Records in respect of both of these elements are important to ensuring effective implementation.
Linking the retention period to the period on which the due diligence procedures were carried out	Where jurisdictions have linked the retention period to the date when the due diligence procedures were carried out (and the records created or obtained), this has resulted in a shorter retention period than that required by the Standard (five years from the end of the period when the Reporting Financial Institutions must report the information). If the retention period is linked to the date on which the due diligence procedures were undertaken, records would not be required to be kept beyond the first five years of reporting even where the account remains reportable in any subsequent periods. This approach therefore leaves a significant deficiency in a jurisdiction's legal framework and in its effective implementation.
Linking the retention period to the last day on which the account was open	Where jurisdictions have linked the retention period to the last date on which the account was open, it often results in a shorter retention period than required by the Standard. For example, if an account was closed on 15 January 2020, and the retention was specified for six years from the last day on which the account was open, records would be required to be kept until 15 January 2026. However, if the reporting date for the jurisdiction is 31 May, the Standard would require reporting on 2020 by 31 May 2021 and therefore the records to be kept until 31 May 2026. A seven year or longer retention period following account closure would however address this issue.
Not specifying the date of commencement of the retention period	Jurisdictions need to set from when the retention period would start, so that there are clear rules for the Reporting Financial Institutions on the length of the record-keeping obligations.

6.2.4. Access and information gathering powers

What is required?

Jurisdictions must have rules in place to ensure access by the relevant authorities to the information and records that Reporting Financial Institutions are required to retain in respect of their CRS obligations. These information access and gathering powers are a key element of a jurisdiction's administrative compliance framework to ensure effectiveness of the implementation of the Standard domestically. They must be available to the appropriate authority or authorities responsible for administering and enforcing the CRS legislative framework, and cover all relevant persons and information.

Why is it important?

Access and information gathering powers are needed to allow the competent authority (or other designated authorities) to carry out activities, as part of its administrative compliance framework to ensure that Reporting Financial Institutions have fulfilled their due diligence and reporting obligations.

Such activities may include verifying self-certifications, AML/KYC documentation or internal procedures to ensure that a Reporting Financial Institution correctly identified all Reportable Accounts; or reviewing IT systems to ensure that all information in respect of these accounts has been correctly reported.

How can the requirement be implemented?

Jurisdictions should have in place effective enforcement provisions to compel the production of information and records for compliance purposes.

In practice, jurisdictions may often request that information be provided in paper or electronic format, including remotely as part of a desk-based audit. However, as some information may only be practically obtained onsite, an effective power to verify compliance should allow for information to also be obtained at the premises of any Financial Institution. This may require a power to ensure access to the relevant premises (see Table 19 on some common pitfalls).

6.2.5. Penalties

What is required?

A jurisdiction must have rules and administrative procedures in place to ensure compliance with the reporting and due diligence procedures. In practice, this includes sanctions available that act as an effective deterrent to non-compliance and that can be imposed when non-compliance is identified.

While the end objective of such measures is to ensure that Reporting Financial Institutions file correct CRS returns including all required information, sanctions will be needed in respect of a number of different compliance aspects to

Table 19. **Access powers – Common pitfalls**

Reliance on incompatible existing powers	Tax and AML/CFT authorities typically already have information access and gathering powers for fulfilling their primary functions. However, existing legislation can limit these powers to the purposes of verifying compliance with a particular tax or AML/CFT Act. These access powers may not always cover all Entities. In cases where the CRS provisions have been implemented in separate legislation, this has been found to prevent the application of access powers for purposes of ensuring compliance with the CRS obligations.
Powers not allocated to relevant authority	As the purpose of accessing information and records is to verify compliance, where this has not been allocated to the authority(ies) responsible for verifying compliance, this has resulted in a deficiency in the implementation of the Standard.
Relevant authorities unable to share information	Where more than one authority is involved in ensuring compliance with the CRS legislation, they must all have access to the relevant documents and information. In the absence of all authorities being allocated the necessary powers, where a jurisdiction has not had a legal and effective means to obtain and share information between authorities, this can result in a deficiency in the effective implementation of the Standard.

ensure that the Standard is being effectively implemented. Penalties and/or other sanctions should be available in the legal framework for any of the following compliance failures:

- failure to maintain and provide access to records
- failure to file (including late filing)
- making a false or misleading statement (e.g. filing an incorrect return or submitting a false self-certification)
- failing to carry out the required due diligence.

Access and record keeping

The power to access information or to demand the provision of information is set out under Subsection 6.3.4 of the toolkit. In order to ensure that Financial Institutions maintain information and produce it on request to the tax authority, these powers must be supported by appropriate penalties on persons who fail to comply.

Failure to file and late filing

The obligation on Reporting Financial Institutions to report the CRS data to the tax authority by a specified date is only sustainable when backed by a penalty for failure to do so. As late filing may prevent the jurisdiction from meeting its commitment to exchange all CRS data by 30 September with partner jurisdictions, the penalty provision introduced must cover both non-filing and late filing.

When introducing this penalty provision, jurisdictions should take care to cater for the likelihood that multiple Reportable Accounts are likely to be reported within a single filing. The size of the total penalty imposed should reflect the seriousness of the failure. Jurisdictions should therefore reflect on whether the penalty should increase to reflect the number and/or monetary size of the Reportable Accounts which were not reported in order to ensure that the penalty retains a deterrent effect. One way that jurisdictions can achieve this is by imposing a penalty per Reportable Account or a penalty in respect of the balances or other amounts that were not reported.

False or misleading statements

In order to ensure that Financial Institutions, Account Holders and Controlling Persons provide correct information as required, jurisdictions should have a penalty to sanction failures to make true and correct statements. This should cover:

- the accuracy of the information filed by Reporting Financial Institutions, including
  - within the CRS information filed
  - information provided upon request in the context of compliance activities
- the accuracy of statements made by persons completing self-certifications.

In these cases, jurisdiction may wish to distinguish between behaviours leading to false or misleading statements by providing for substantially greater penalties in cases of careless or deliberate behaviour as opposed to where reasonable care has been taken.

Failing to carry out due diligence and to obtain self-certifications

Reporting Financial Institutions will have reporting obligations only where the due diligence has identified Reportable Accounts (or where there is a nil filing requirement). Jurisdictions should therefore ensure that penalties can be applied to failures in carrying out CRS due diligence which are independent of any penalty applicable on failures to report correctly.

Obtaining self-certifications when required can be considered to be part of the overall due diligence requirements and jurisdictions may choose to cover this with a single penalty for any failure to conduct required due diligence. Alternatively, a jurisdiction may choose to have distinctly separate penalties for each of these elements of non-compliance.

As is the case for reporting failures, the penalty should be commensurate with the scope of the failure. If a due diligence failure, such as a failure to obtain a valid self-certification when required, has affected multiple accounts, a penalty per account affected by the failure may be appropriate.

How can the requirement be implemented?

Can a jurisdiction rely on existing legislation?

An initial consideration is whether the jurisdiction needs to introduce CRS specific penalties, or whether

existing penalties in the jurisdiction (for example, in tax law) would already cover non-compliance. This should be examined very carefully for each type of non-compliance. Generally, jurisdictions which have initially relied fully on existing penalties legislation have been found to have deficiencies because they do not cover all possible aspects of CRS non-compliance. For example, a penalty that relies on a domestic tax connection will not work for CRS non-compliance because there is generally no domestic tax involved for the Reporting Financial Institution or the Reportable Person.

A jurisdiction may find that it needs to create specific penalty provisions to cover every type of CRS non-compliance. Alternatively, it may find that some aspects are covered by existing penalties and some will require a new, specific penalty. This hybrid approach has most commonly been used where jurisdictions continue to rely on a sanction in their wider legal framework that can be applied to a person making a false statement in a self-certification, such as by applying a general fraud provision.

Fraud provisions and similar sanctions in respect of providing false self-certifications must be carefully analysed by the jurisdiction to ensure that they can be relied upon in all required circumstances. In particular, the sanction provision needs to meet all three of the following requirements:

- The sanction can be applied to all forms of self-certifications, noting that self-certifications can be provided in various forms (e.g. in paper, electronically, or in a voice recording) and they can be signed or positively affirmed.
- The sanction is not dependent on incorrectly acquiring property or some other gain (which may not be the case following the provision of a false self-certification).
- The sanctions are applicable to all Account Holders and Controlling Persons, including all domestic and foreign individuals and Entities.

Penalty amounts

The appropriateness of penalty levels is context specific, both with respect to a jurisdiction's wider compliance framework and what is effective in practice in the wider context of each jurisdiction. However, there should be a level of comfort that the applicable penalties are sufficient to help ensure compliance.

It is not possible to be prescriptive on the required levels of penalties or to develop a level of penalty that could be said to be effective for every jurisdiction. It is nevertheless possible to identify penalties that are very likely to be ineffective. A penalty that is essentially negligible will provide no comfort that it will be effective in ensuring an effective implementation in the Standard. An important consideration in this regard could be a comparison to the applicable penalties/sanctions for other comparable domestic tax matters.

Jurisdictions are also able to have non-financial sanctions available to supplement the financial penalties, such as actions that would affect a Financial Institution's license to provide services. However, if these sanctions are available they should not be the sole sanction relied upon. In practice, if the only sanction available is excessively disproportionate to the non-compliance, it can become ineffective through an administrative reluctance to impose it.

Table 20 presents some of the issues identified in the peer review process.

Effective implementation

Penalties must be effectively applied in case of non-compliance. Therefore, two elements should be considered to ensure the effectiveness of the sanction framework.

- **Application procedures:** Jurisdictions should consider how their penalties will be imposed in practice to ensure that they remain effective. If penalties can only be imposed by a court following conviction, they have sometimes been found to be burdensome to apply and as a consequence rarely or never used. Many jurisdictions have therefore opted for penalties that can be imposed administratively. Such penalties could be lower in amount, with an escalation path to court imposed penalties for more serious or repeated non-compliance.

- **Discretion and remission:** Many jurisdictions will have, in some form, an administrative or legal power in the hands of the tax official or Commissioner to choose whether to impose a penalty, the amount of the penalty, or to remit some or all of a penalty in appropriate circumstances. The existence of such powers is not at face value an issue that will impact on the effectiveness of the penalty provisions and can in practice allow for a more equitable system when circumstances, compliance records or behaviour are taken into account. Effectiveness of implementation is measured over time. Likewise, no adverse view is taken of jurisdictions who do not have or do not use such discretionary powers.

In addition, alongside the introduction of penalties in the domestic legislative framework, jurisdictions can be mindful of having appropriate appeals procedures as well as systems to record and collect the penalties. There are no special requirements in these areas for CRS purposes.

6.2.6. Anti-circumvention

What is required?

Jurisdictions must have in place rules to prevent any persons, including Financial Institutions and intermediaries, from adopting practices to circumvent (or avoid) the reporting and due diligence procedures. Such rules are expected to address all of the example situations set out in Box 11 and should:

- prevent such practices from taking place
- ensure that such practices are not legally effective if carried out
- ensure that information is sent to the relevant jurisdiction when such practices are detected.

Table 20. **Penalties – Common pitfalls**

Existing penalties legislation do not cover all areas of CRS non-compliance	Where existing penalties in the tax framework have been relied upon, they have been considered ineffective where a domestic tax connection is needed. This is because Reporting Financial Institutions and Reportable Persons will not always have a domestic tax connection. Furthermore, penalty amounts linked to the unpaid tax revenue will not be applicable in any of the aforementioned CRS compliance failures. Reliance on existing penalties and sanctions in the AML/CFT framework, particularly in respect of CRS due diligence requirements, have also been considered ineffective. This is because while information obtained under AML/KYC procedures may be relied upon, most of the due diligence requirements under Sections II to VII are separate from the Financial Institutions' AML/CFT obligations.
Absence of an effective penalty on persons that provide false self-certifications	An ability to penalise the provision of false self-certifications is an area which had initially been overlooked by a number of jurisdictions. Existing provisions in respect of fraud which do not meet the aforementioned requirements have resulted in deficiencies. Jurisdictions should make sure that any power to introduce penalties included in primary legislation allows such a penalty to be introduced on Reportable Persons (Account Holders and Controlling Persons) and that such a power is not restricted to introducing penalties in respect of Reporting Financial Institutions and their due diligence and reporting obligations.
Only having a penalty in respect of filing obligations and providing inaccurate information	Some jurisdictions initially relied on penalties for failing to report an account as a substitutable penalty for failing to carry out due diligence on the basis that the failure to carry out due diligence is only a concern when it results in a failure to report an account. However, this approach does not meet the requirements of the Standard as the obligation to carry out due diligence should be carried out correctly on all accounts irrespective of whether each account is ultimately found to be reportable or becomes reportable at a later time.

Why is it important?

It is important to distinguish between non-compliance with the due diligence and reporting rules in Sections I to VII from attempts to circumvent such rules. The need for such anti-circumvention measures reflects that even if jurisdictions fully implement the reporting and due diligence rules, persons using offshore accounts to facilitate tax evasion and avoidance may seek ways to avoid due diligence being carried out on their investments or otherwise prevent information from being reported to their jurisdiction of residence. This avoidance may be facilitated by Financial Institutions, intermediaries or any other persons seeking to prevent an account from becoming reportable. Alternatively, avoidance may be undertaken by Entities seeking to prevent themselves from becoming Reporting Financial Institutions.

Circumvention practices could involve the practice of moving assets, entering into artificial transactions, or restructuring affairs to prevent the information from being reported. Such practices may also be undertaken as part of marketed schemes which are akin to traditional tax avoidance schemes.

Marketed schemes to circumvent the rules would require the involvement of either the Financial Institution itself or the involvement of intermediaries or other persons, such as a financial, tax or legal advisors. For this reason, jurisdictions must have rules in place which can cover the adoption of such practices by any person, including the Account Holder, Controlling Persons, intermediaries and Financial Institutions.

How can the requirement be implemented?

The most effective approach which jurisdictions can adopt to address circumvention of the CRS obligations is the null and void approach. Jurisdictions can also introduce further measures such as mandatory disclosure regimes to supplement this approach.

Null and void approach

A null and void rule has a similar effect to general anti-avoidance rules used for tax purposes. If a person enters into an arrangement or engages in a practice where one of the main purposes is to circumvent the due diligence and reporting rules, the rule requires that that the due diligence and reporting obligations must still be complied with as if the circumvention had never taken place.

Box 11. **Examples of situations where it is expected that an anti-circumvention rule would apply**

The Commentary under Section IX outlines the following examples where it is expected that the anti-circumvention rule will apply.

Example 1 (Shift Maintenance of an Account)

A Reporting Financial Institution advises a customer to maintain an account with a Related Entity in a non-Participating Jurisdiction that enables the Reporting Financial Institution to avoid reporting while offering to provide services and retain customer relations as if the account was maintained by the Reporting Financial Institution itself. In such a case, the Reporting Financial Institution should be considered to maintain the account and have the resulting reporting and due diligence requirements.

Example 2 (Year-end amounts)

Financial Institutions, individuals, Entities or intermediaries manipulate year-end amounts, such as account balances, to avoid reporting or being reported upon.

Example 3 (Park Money with Qualified Credit Card Issuers)

Individuals or Entities park balances from other Reportable Accounts with Qualified Credit Card Issuers for a short period at the end of the year to avoid reporting.

Example 4 (Electronic records and computerised systems)

A Reporting Financial Institution deliberately does not create any electronic records (such that an electronic record search would not yield any results) or maintains computerised systems artificially dissociated (to avoid the account aggregation rules).

Source: CRS Commentary on Section IX, paragraph 5.

In practice, this could mean that if a Financial Institution has been party to (or aware of) the circumvention, it will immediately have to disregard the circumvention practices when carrying out due diligence and reporting. In other cases, where circumvention has been identified by the tax administration, for example through a mandatory disclosure regime, the Financial Institution would be required to disregard these practices upon being notified of the circumvention.

In short, when a practice is carried out by persons to circumvent the CRS obligations, such practice will be considered null and void, and failure to disregard the circumvention should result in the application of the applicable penalty for non-compliance. The focus of the null and void approach is to ensure that circumvention can be addressed, rather than simply detection of circumvention.

Mandatory disclosure regimes

Mandatory disclosure regimes can offer an effective measure to assist jurisdictions in identifying circumvention practices and offer an effective tool to help deter circumvention. However, because their focus concerns the identification of circumvention practices, they must be combined with further measures in the legislative framework, such as the null and void approach, to ensure that the circumvention is prevented and that the correct information is reported to the relevant jurisdiction.

CRS avoidance mandatory disclosure regimes, including the OECD *Mandatory Disclosure Rules for CRS Avoidance Arrangements and Opaque Offshore Structures*,[65] often have the purpose of informing both the tax authority of the jurisdiction where the avoidance was reported as well as the tax authority of the jurisdiction whose tax resident is party to the circumvention. While the exchange of this information to the tax resident's jurisdiction is important, a sending jurisdiction should also actively use the information reported before it is sent to be effective in deterring circumvention. The jurisdiction can then undertake the necessary compliance activity (such as sanctions or application of the null and void approach) to ensure that the correct CRS information is reported.

Table 21 summarises certain common pitfalls identified in the implementation of the anti-circumvention rule.

6.2.7. Overriding pre-existing secrecy or confidentiality provisions

What is required?

The implementation of the Standard in any jurisdiction must work in practice and not be inhibited by any other legislative provisions. Some jurisdictions have client confidentiality or "banking secrecy" provisions in their legislative framework, including within civil and/or

65. OECD (2015), Mandatory Disclosure Rules, Action 12 - 2015 Final Report, op. cit.

Table 21. **Anti-circumvention – Common pitfalls**

Reliance on the sanctions applicable for incorrect due diligence and reporting	There is a distinction between failure to comply with due diligence and reporting rules, and measures undertaken to circumvent them. Therefore the sanctions applicable for incorrect due diligence or reporting do not address the circumvention issue and would be unlikely to apply to the examples in Box 11.
Measures only applicable to Financial Institutions	Anti-circumvention measures must not only apply to Financial Institutions, but also to any other persons (individual or Entity), which could include intermediaries, Account Holders and Controlling Persons even though such persons do not have due diligence or reporting obligations under the CRS legislation.
Reliance only on mandatory disclosure rules	While mandatory disclosure rules would identify circumvention practices, they would not on their own prevent practices from taking place or address the practices to ensure that the correct information is reported.
Reliance on sanctions in respect of fraud or forgery	The circumvention examples set out in the Commentary would not typically be considered an act of fraud or forgery, therefore such sanctions are unlikely to amount to a measure to prevent circumvention.

penal codes. In such cases, jurisdictions must ensure that these provisions are overridden, and that primacy is given to the CRS legislation in the context of reporting the relevant information for CRS-AEOI purposes.

Why is it important?

As a tool to ensure transparency for tax purposes, the Standard is incompatible with legislative provisions intended to guarantee client (Account Holder or Controlling Person) discretion or secrecy vis-à-vis the client's respective tax authority.

While jurisdictions will seek to ensure that some confidentiality provisions remain in place to prevent the disclosure of information to unauthorised persons, no provision should obstruct Financial Institutions from carrying out the due diligence requirements or from reporting the required information to the tax authority for the purposes of onward exchange under the CRS.

For this reason, it is important that:

- primacy is given to the CRS legislation introduced so that it overrides any conflicting confidentiality or secrecy provisions
- persons obligated to report the CRS information (Financial Institutions and their personnel) are relieved of any liability that existing legislation would otherwise impose for this disclosure of information.

CRS data remains protected by domestic provisions relating to tax secrecy as well as confidentiality provisions of the exchange agreement between the sending and receiving jurisdictions (see Box 12).

How can the requirement be implemented?

In all cases, jurisdictions will have to determine the approach needed based on their circumstances and any pre-existing and potentially conflicting rules.

Most jurisdictions implementing CRS legislation do not need to take any specific action to ensure that the CRS legislation does not conflict with existing confidentiality provisions. This is the case where the introduction of new legislation by default overrides any existing legislative provisions.

Where jurisdictions believe that specific action might be needed, available approaches include:

- **a specific override clause** in the CRS legislation to ensure the CRS requirements take primacy over any existing, conflicting legislation. Even where such an override clause is not required in the jurisdiction as there is no clear conflict, jurisdictions may wish to include it to offer clarity and assurance to those in the financial industry with reporting obligations.
- **amendments to existing civil or penal codes** if the provisions of such codes on confidentiality or secrecy remain in conflict with the CRS legislation introduced. This could be the case where a jurisdiction's penal code includes a criminal liability on any person who discloses information in respect of financial accounts.

6.2.8. Strong measures to ensure self-certifications are always obtained

What is required?

A fundamental element of the CRS due diligence rules is that a valid self-certification must be obtained for all New Accounts. Where the CRS and its Commentary have been incorporated into a domestic legislative

Box 12. **Introducing confidentiality provisions**

Jurisdictions are expected to have measures in place to protect the confidentiality and appropriate use of the information to be sent automatically to exchange partners, and this is subject to an assessment under the CR 3 of the ToR as part of safeguarding the lifecycle of the data.

Most jurisdictions have in place existing confidentiality provisions in respect of taxpayer information or information obtained by government officials. Jurisdictions may however find additional clarity within their CRS legislation a helpful addition to any existing legislation.

The model rules based on the reference method in Annex 3 include provisions under Section 7(2) and (3) on confidentiality to ensure that persons such as officials or employees of the tax administration handle the information received from a Reporting Financial Institution in the course of their duties in a confidential manner.

framework in full, alongside appropriate relevant penalties, then by default no further legislative requirements are needed.

FAQ 22 provides jurisdictions with the option for a very limited relaxation to this requirement if a jurisdiction deems it necessary. Generally the Standard requires collection and validation of a self-certification upon account opening. However, FAQ 22 refers to the possibility (it is not required) for a jurisdiction to permit "day two" procedures for the collection or validation of self-certifications in exceptional circumstances (i.e. where a self-certification cannot be collected and/or validated upon account opening). Examples of such exceptional circumstances are described in FAQ 22:

> *There are a limited number of instances, where due to the specificities of a business sector it is not possible to obtain a self-certification on 'day one' of the account opening process, for example where an insurance contract has been assigned from one person to another or in the case where an investor acquires shares in an investment trust on the secondary market.*

If a jurisdiction chooses to permit "day two" procedures, FAQ 22 sets out the clear expectation that the jurisdiction must have in place strong measures to ensure that self-certifications are ultimately collected and validated (within 90 days from the opening of the account) whenever a Reporting Financial Institution uses the procedures.

How can it be implemented?

The FAQ explains that what constitutes strong measures will vary from jurisdiction to jurisdiction but ultimately it is the success of the strong measures that is important. The crucial test for determining what can qualify as a "strong measure" is whether it has a strong enough impact on Financial Institutions and/or Account Holders and Controlling Persons to effectively ensure that self-certifications are obtained and validated in accordance with the rules set out in the CRS. The measure is described in terms of being "strong" because it may need to be stronger than the standard measures that ensure collection on opening of an account, because obtaining a self-certification after opening the account can be more difficult.

Strong measures could include:

- providing Reporting Financial Institutions with the ability to compel the provision of self-certifications including through the ability to suspend or close the account
- compelling the Reporting Financial Institutions with a direct obligation to suspend or close the account
- applying a sufficiently persuasive penalty on the Reporting Financial Institution that has not collected a self-certification as part of "day two" procedures
- imposing a penalty on the Account Holder, either directly or through collection from the Reporting Financial Institution that is permitted to recover the amount from the Account Holder.

Since the allowance of the "day two" procedures in FAQ 22 provides a relaxation of the default position in the Standard, jurisdictions that have opted to provide for it have generally done so through guidance material rather than explicitly including it in law. The guidance can be non-binding and may reproduce the FAQ in full, reference the FAQs as a whole, or reference FAQ 22 specifically.

If a jurisdiction opts to allow for "day two" procedures, it needs to consider any further adjustments necessary to the legal framework to provide for measures that ensure self-certifications are obtained. Such measures may have to be introduced by adapting the domestic CRS legislation as they are not provided for in the CRS and its Commentary and will very likely need to be included in a binding legislative instrument such as regulations or binding guidance.

6.3. STEP 3: WHAT OPTIONAL PROVISIONS CAN BE IMPLEMENTED?

The precise and inflexible nature of the due diligence and reporting requirements on Financial Institutions helps to ensure a level playing field across all jurisdictions which have implemented the Standard, limits the opportunities for circumvention, and ensures that receiving jurisdictions can expect consistency in the information received from sending jurisdictions.

However, the CRS includes a number of optional provisions to allow jurisdictions to adjust the requirements to reflect some of their specific circumstances and to give some flexibility to Financial

Institutions in the application of the due diligence requirements.[66] Jurisdictions can therefore choose to introduce these optional provisions into their domestic legislative framework.

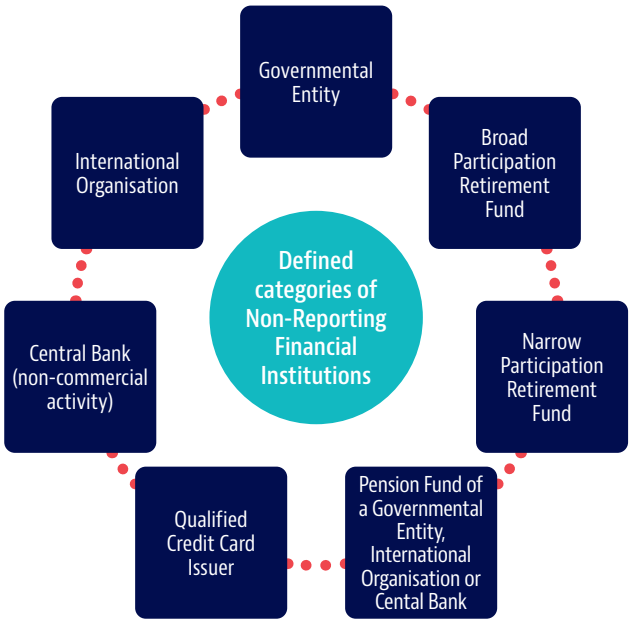
6.3.1. Jurisdiction-specific Non-Reporting Financial Institutions

What are they and what do they allow for?

Non-Reporting Financial Institutions are Financial Institutions that are not required to review their accounts or report information under the Standard. The CRS sets out clearly defined categories of Financial Institutions that are specifically excluded from being required to report information because they are considered to pose a low risk of being used to evade taxes (CRS, Section VIII(B)(1)(a) and (b)) (see Figure 13). In addition to these categories, jurisdictions also have the possibility to define jurisdiction-specific Non-Reporting Financial Institutions, providing they meet certain conditions. This accounts for the fact that there may be certain types of Financial Institutions that present a low risk of being used for tax evasion purposes but that do not completely meet the requirements of the established categories of Non-Reporting Financial Institutions in the CRS.

66. OECD (2018), *Standard for Automatic Exchange of Financial Information in Tax Matters - Implementation Handbook*, op. cit., pp. 15-19.

FIGURE 13. **Defined categories of Non-Reporting Financial Institutions**



Note: These categories of Non-Reporting Financial Institutions are strictly defined in Section VIII(B)(1)(a) and (b) of the CRS and additional guidance is provided in the Commentary.

To be classified as Non-Reporting Financial Institutions, the CRS sets out that these jurisdiction-specific Financial Institutions should fulfil the following conditions (CRS, Section VIII(B)(1)(c)):

i. They represent a low risk of being used for tax evasion purposes.

ii. They have substantially similar characteristics to any of the Entities described in Section VIII(B)(1)(a) and (b) of the CRS.

iii. They do not frustrate the purposes of the CRS.

iv. They are defined in the domestic law as Non-Reporting Financial Institutions.

When can this provision help jurisdictions?

The possibility for jurisdictions to exclude certain Financial Institutions from their reporting obligations is to recognise that, in practice, there may be Financial Institutions that present a low risk of being used for tax evasion purposes due to the particular characteristics of their business or the types of products they offer. This allows each jurisdiction's particular circumstances to be taken into consideration. For example, in some jurisdictions, there might be pension funds that offer pension benefits to former employees of an employer and that operate under certain conditions, such as being subject to government regulations and exempt from certain taxes. In such cases, provided that the funds meet all of the requirements, jurisdictions can opt to include them in a jurisdiction-specific list of Non-Reporting Financial Institutions.

The Global Forum reviews the jurisdiction-specific lists of Non-Reporting Financial institutions to ensure that all of the requirements are met. When using this option, a jurisdiction is expected to have only one list of jurisdiction-specific Non-Reporting Financial institutions (as opposed to different lists for different Participating Jurisdictions) and that it would make such a list publicly available as required under the Standard.

How can the option be implemented?

Any jurisdiction considering introducing a jurisdiction-specific list of Non-Reporting Financial Institutions should reflect on the nature of its financial sector and the types of Financial Institutions that operate there, including through consultation with the financial sector as appropriate. Non-Reporting Financial Institutions will often be Financial Institutions that are subject to governmental regulation, or controlled by Governmental Entities, and that are already required to report information to the tax authorities. Once such Entities have been identified, the jurisdiction should carry out analysis to determine which of these represent a low risk of being used for tax evasion and have substantially similar characteristics to one of the categories of Non-Reporting Financial Institutions set out by the CRS. The financial sector itself might assist in providing the underlying information relevant to identify the suitability of the Entity to be included on the list.

If a jurisdiction decides to provide for a jurisdiction-specific exclusion, the CRS-AEOI standard requires it to be specified in domestic law. Such exclusions have usually been introduced by way of secondary legislation, or have been set out in a Schedule or Annex to the primary legislation. This is the approach followed in the model rules, both the copy out (available on request) and reference (Annex C of the toolkit) methods.

Jurisdictions should also take into account the fact that entities excluded from reporting under their FATCA IGA may not qualify as Non-Reporting Financial Institutions under the CRS (see Box 13).

Practical examples on jurisdiction-specific Non-Reporting Financial Institutions

Pension or retirement funds

The CRS includes three categories of pension or retirement funds that are classified as Non-Reporting Financial Institutions (CRS, Section VIII(B)(1)(b)):

i. Broad Participation Retirement Fund

ii. Narrow Participation Retirement Fund

iii. Pension Fund of a Governmental Entity, International Organisation or Central Bank.

Box 13. **Interaction between the list of jurisdiction-specific Non-Reporting Financial Institutions and the contents of Annex II to the FATCA IGAs**

Annex II to the Model 1 FATCA IGA describes the categories of entities that are excluded from reporting for FATCA purposes. Additionally, Annex II may be modified to include additional Financial Institutions that present a low risk of being used for tax evasion in the US.

Given the similarities between the FATCA IGAs and the CRS, there is likely to be some overlap between the Financial Institutions included in Annex II of the FATCA IGAs and the list of jurisdiction-specific Non-Reporting Financial Institutions for CRS purposes. However, not all Entities included in Annex II to the FATCA IGAs can be classified as Non-Reporting Financial Institutions under the CRS, and jurisdictions should take this into account when drawing up any jurisdiction-specific list. This is because some of the categories of Financial Institutions excluded from reporting for FATCA purposes were not considered as categories of Non-Reporting Financial Institutions under the CRS, for example, Treaty Qualified Retirement Funds, Financial Institutions with a Local Client Base or Local Banks are not excluded from due diligence and reporting under the CRS. FAQ 2 on Section VIII(B) of the CRS includes an explanation of the relationship between the jurisdiction-specific categories of Non-Reporting Financial Institutions in the CRS and the contents of Annex II to the FATCA IGAs.

Jurisdictions should take into account that for a Financial Institution listed in Annex II of the FATCA IGA to be considered a jurisdiction-specific Non-Reporting Financial Institution for CRS purposes, it must fulfil all the conditions set out in Section VIII(B)(1)(c) of the CRS, including having substantially similar characteristics to one of the defined categories of Non-Reporting Financial Institutions set out in the CRS.

Table 22 describes the characteristics for a fund to be classified under each of the categories.

Pension or retirement funds most commonly listed under jurisdiction-specific Non-Reporting Financial Institutions lists are Broad Participation Retirement

Table 22. **Categories of pension or retirement funds**

<table>
<tr><th>Broad Participation Retirement Fund</th><th>Narrow Participation Retirement Fund</th><th>Pension Fund of a Governmental Entity, International Organisation or Central Bank</th></tr>
<tr><td colspan="2">Fund established to provide retirement, disability, or death benefits, or any combination thereof, to beneficiaries that are current or former employees (or persons designated by such employees) of one or more employers in consideration for services rendered, provided that:</td><td rowspan="2">Fund established by a Governmental Entity, International Organisation or Central Bank to provide retirement, disability, or death benefits to beneficiaries or participants that are current or former employees (or persons designated by such employees).

For beneficiaries that are not current or former employees, the benefits provided to such beneficiaries are in consideration of personal services performed for the Governmental Entity, International Organisation or Central Bank.</td></tr>
<tr><td>● Entitlement of any beneficiary to more than five percent of the fund's assets is prohibited.

● The fund is subject to government regulation and provides information reporting to the tax authorities.

● The fund satisfies at least one of the following:
– It is exempted from tax on investment income, or taxation of such income is deferred or taxed at a reduced rate.
– It receives at least 50% of its total contributions from the sponsoring employers.
– Distribution or withdrawals from the fund are allowed only upon the occurrence of specified events related to retirement, disability or death, or penalties apply to distributions or withdrawals made before such specified events.
– Contributions by employees to the fund are limited by reference to earned income of the employee or may not exceed USD 50 000 annually</td><td>● The fund has fewer than 50 participants.

● The fund is sponsored by one or more employers that are not Investment Entities or Passive NFEs.

● The employee and employer contributions to the fund are limited by reference to earned income and compensation of the employee, respectively.

● Participants that are not residents of the jurisdictions where the fund is established are not entitles to more than 20% of the fund's assets.

● The fund is subject to government regulation and provides information reporting to the tax authorities.</td></tr>
</table>

Funds. Many jurisdictions have funds dedicated to providing retirement, disability or death benefits to a particular group of employees or former employees of an employer. There may also be funds dedicated to providing pension benefits to self-employed workers of specific professions. These funds are generally subject to supervision under the social security regime of the jurisdiction (e.g. in terms of contributions and benefits provided) and have reporting obligations to the tax authorities.

Where not all of the requirements to be classified as a Broad Participation Retirement Fund are fully met, substantially similar characteristics that assure an

equivalent level of low risk must be fulfilled. Examples of this are:

i. where there is no requirement to have an employment connection to be a beneficiary of the fund, individual participants should not have an ability to control the funds or use the fund for personal purposes

ii. the fund can provide benefits other than for retirement, disability or death as long as the funds can only be accessed in restricted circumstances, such as after a very long period of time.

Entities that are not Financial Institutions

A common pitfall has been observed when jurisdictions have provided for a category of Non-Reporting Financial Institution which includes or would frequently include entities that are in fact not Financial Institutions under the Standard. Examples have included asset leasing companies, debt factoring companies and businesses solely engaged in currency exchange.

Assessment of all jurisdiction-specific Non-Reporting Financial Institutions

Jurisdiction-specific Non-Reporting Financial Institutions are assessed by the Global Forum to ensure that they meet all the requirements of the CRS (see Subsection 2.4.2 of the toolkit). The review examines:

i. whether the Entity meets the definition of a Financial Institution

ii. whether the Financial Institution presents a low risk of being used for tax evasion

iii. under which category of the defined exclusions of the CRS the Financial Institution falls based on its characteristics

iv. which characteristics are not met but have substantially substitute characteristics that ensure the Financial Institution presents an equivalent level of low risk.

Where jurisdictions have introduced jurisdiction-specific Non-Reporting Financial Institutions that do not meet all of these requirements, this has been considered to be a deficiency in the legal framework resulting in a recommendation or note.

6.3.2. Jurisdiction-specific Excluded Accounts

What are they and what do they allow for?

Excluded Accounts are accounts for which Financial Institutions are not required to carry out diligence on or to report on. The CRS sets out clearly defined categories of what meets the definition of an Excluded Account (Section VIII(C)(17)(a) through (f)) (see Figure 14). In addition to these defined categories, jurisdictions also have the possibility to introduce jurisdiction-specific Excluded Accounts. This is to account for the fact that there may be certain types of accounts in a jurisdiction that present a low risk of being used for tax evasion but that do not completely fulfil the requirements of the established categories set out by the CRS. Jurisdictions may provide for jurisdiction-specific Excluded Accounts, but it is not a requirement to do so.

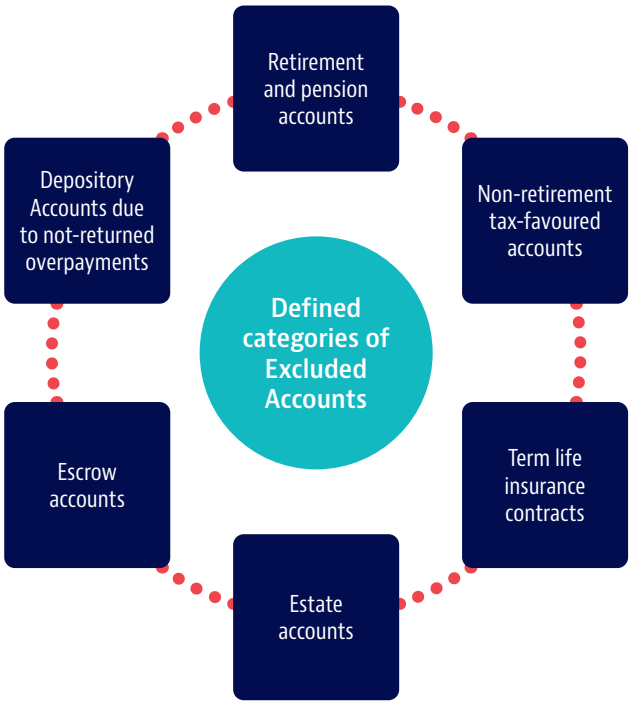
To be classified as such, these jurisdiction-specific accounts should fulfil the following conditions (CRS, Section VIII(C)(17)(g)):

- They pose a low risk of being used for tax evasion.
- They have substantially similar characteristics to any of the defined Excluded Accounts described in Section VIII(C)(17)(a) through (f) of the CRS.
- They do not frustrate the purposes of CRS.
- They are defined in the domestic law as Excluded Accounts.

When can this provision help jurisdictions?

The ability to exclude certain jurisdiction-specific accounts is intended to ease the burden on Financial Institutions in having to review and report accounts that in practice present a low risk of being used for tax evasion purposes. This allows each jurisdiction's particular circumstances to be taken into consideration. For example, some jurisdictions might have certain pension or savings accounts that pose a low risk of being used for tax evasion because they are subject to strict requirements on the amounts contributed by the Account Holder as well as residency requirements. Providing they meet all of the above-mentioned requirements, jurisdictions can choose to include them in a jurisdiction-specific list of Excluded Accounts.

FIGURE 14. **Defined categories of Excluded Accounts**



Note: These categories of Excluded Accounts are strictly defined in Section VIII(C)(17)(a) through (f) of the CRS and additional guidance is provided in the Commentary.

The Global Forum reviews the jurisdiction-specific lists of Excluded Accounts to ensure that all of the requirements are met. When using this option, a jurisdiction is expected to make such a list publicly available.

How can the option be implemented?

Any jurisdiction considering introducing a jurisdiction-specific list of Excluded Accounts should reflect on the types of financial accounts (products) commonly offered by its Financial Institutions, consulting with the financial sector as appropriate. These will typically be accounts which meet a specific definition set out in regulation because of particular characteristics. Such accounts are often defined in legislation because they are tax-favoured, or where contributions are incentivised, such as for future retirement saving.

Once such accounts have been identified, the jurisdiction should carry out analysis to determine which of these represent low risk of being used for tax evasion and have substantially similar characteristics to one of the categories of Excluded Accounts set out by the CRS. The financial sector itself might assist in providing the underlying information relevant to identifying potential Excluded Accounts.

If a jurisdiction decides to provide for a jurisdiction-specific exclusion, the Standard requires it to be specified in domestic law. These have usually been introduced by way of secondary legislation, or have been set out in a Schedule or Annex to the primary legislation. This is the approach followed on the model rules, both the copy out (available on request) and reference (Annex C of the toolkit) methods.

Practical examples on jurisdiction-specific Excluded Accounts

Accounts held by a group of owners, for the purpose of paying the ongoing expenses of a condominium or housing cooperative

A Financial Account held by or on behalf of a group of owners or by the condominium company for paying the expenses of the condominium or housing cooperative, usually denominated as "condominium accounts", have often been included in jurisdiction-specific lists of Excluded Accounts.

These accounts can fall within the exclusion of non-retirement tax-favoured accounts (CRS, Section VIII(C)(17)(b)) provided that they satisfy the following conditions:

i. It is regulated in domestic law as a specific account for covering the costs of a condominium or housing cooperative.

ii. The account or the amounts contributed and/or kept in the account are tax-favoured.

iii. The amounts in the account may only be used to pay for the expenses of the condominium or housing cooperative.

iv. No single owner can annually contribute an amount that exceeds USD 50 000.

Where some of the above requirements are not met, for example if the account is not tax-favoured or contributions are not limited to USD 50 000, the condition of having substantially similar characteristics

that assure an equivalent level of low risk needs to be fulfilled. Domestic specificities are taken into consideration. These substantially similar characteristics could be:[67]

i. No more than 20% of the annual and total contributions due in the year being attributable to single person.

ii. The account being operated by an independent professional.

iii. The amounts of the contributions and the use of the money being decided by agreement of owners in accordance with the condominium's or housing cooperative's constituting documents.

iv. Disallowing withdrawals from the account for purposes other than the expenses of the condominium or housing cooperative.

Retirement or pension accounts

Jurisdictions have often included retirement or pension accounts in their jurisdiction-specific lists of Excluded Accounts. These accounts are maintained to receive retirement or pension benefits (including disability or death benefits).

These accounts can fall under the exclusion of retirement or pension accounts (CRS, Section VIII(C)(17)(a)) provided that they satisfy the following conditions:

i. The account is subject to regulation as a personal retirement account.

ii. The account is tax-favoured.

iii. Information reporting is required to the tax authorities with respect to the account.

iv. Withdrawals are conditioned on reaching a specified retirement age, disability, or death, or penalties apply to withdrawals made before such events.

v. Either (i) annual contributions are limited to USD 50 000 or less, or (ii) there is a maximum lifetime contribution limit to the account of USD 1 million or less.

Some common pitfalls have been observed where jurisdictions have incorporated pension accounts to the jurisdiction-specific list of Excluded Accounts but where the characteristics of the accounts were not considered to be substantially similar to the ones required by the CRS. Examples of these have been where:

i. There is no obligation to report information related to the financial activity and balance of the account to the tax authority.

ii. The penalties applicable to early withdrawals were only a different tax treatment for the purposes of calculating the income tax on the interest or gains accrued to the account.

In these cases, a recommendation has been made for the jurisdiction to remove the exclusion from the jurisdiction-specific list of Excluded Accounts.

Dormant accounts

It is common for jurisdictions to provide an exclusion for dormant accounts. While these are not included as one of the standard exclusions in Section VIII(C)(17)(a) through (f), they can be included as a jurisdiction-specific Excluded Account. Dormant accounts is a category included in the Commentary as an example that jurisdictions could incorporate and many have done so. However, in order to ensure that the exclusion is accepted as low-risk in accordance with Section VIII(C)(17)(g), care should be taken to ensure that a dormant account for the purpose of this exclusion is specified in accordance with the criteria described in the Commentary.[68] Specifically it must substantially satisfy the following conditions to be excluded:

i. The account is a Depository Account.

ii. The annual balance does not exceed USD 1 000.

iii. The Account Holder has not initiated a transaction with regard to the account or any other account held by the Account Holder with the Reporting Financial Institution in the past three years.

iv. The Account Holder has not communicated with the Reporting Financial Institution regarding the account or any other account held with the Reporting Financial Institution in the past six years.

67. See FAQ 10 on Section VIII(C) of the CRS.

68. See FAQ 3 on Section VIII(C) of the CRS.

Some common pitfalls that have been observed where jurisdictions have excluded dormant accounts but failed to provide a limit on the balance, or to specify a limit substantially greater than USD 1 000, or failed to include the additional conditions for an absence of transactions and communication for the required periods.

Other examples of Excluded Accounts

Several other examples of acceptable Excluded Accounts can be found at paragraph 103 of the Commentary on Section VIII.

Assessment of all jurisdiction-specific Excluded Accounts

Jurisdiction-specific Excluded Accounts are assessed by the Global Forum to ensure that the requirements of the CRS are met (see Subsection 2.4.2 of the toolkit). The review examines:

i. whether the account would meet the definition of Financial Account were it not excluded

ii. whether the account represents a low risk of being used for tax evasion

iii. under which category of the defined exclusions of the CRS the account falls based on its characteristics

iv. which characteristics are not met but have substantially substitute characteristics that assure an equivalent level of low risk.

Where jurisdictions have introduced jurisdiction-specific Excluded Accounts that do not meet all of these requirements, this has been considered to be a deficiency in the legal framework resulting in a recommendation or note.

6.3.3. Alternative approach to calculating account balances

The CRS and its Commentary foresee the possibility of allowing jurisdictions to permit Reporting Financial Institutions to report the average balance or value of their Reportable Accounts as opposed to the balance or value of the account as at the end of the calendar year. This option was made available to jurisdictions that already require Financial Institutions to report that way. As this approach is not facilitated under the CRS MCAA, it is not considered further within this toolkit.

6.3.4. Use of reporting period other than calendar year

What is it and what does it allow for?

Under the CRS, the information to be reported can be information in respect of the relevant calendar year or another "appropriate reporting period". This allows jurisdictions to permit their Reporting Financial Institutions to report information on a reporting period other than the calendar year.

In determining what "appropriate reporting period" means, reference must be made to the meaning that the term has at that time under each jurisdiction's reporting rules, which must be consistently applied for a reasonable number of years. Examples of other "appropriate reporting period" include:

- the period between the most recent contract anniversary date and the previous contract anniversary date (e.g. in the case of a Cash Value Insurance Contract)
- a fiscal year other than the calendar year.[69]

The "appropriate reporting period" used by an implementing jurisdiction should refer to a period that has been consistently applied for a reasonable number of years.

When can this provision help jurisdictions?

The use of other reporting period is an option that has been widely adopted by jurisdictions as it is considered a simplified approach for Financial Institutions to collect the information that needs to be reported under the CRS. Jurisdictions have adopted it where their fiscal (tax) year is not a calendar year and where reporting requirements for domestic purposes mean that Financial Institutions are already collecting and reporting information in respect of that fiscal year.

Where jurisdictions do use the calendar year as their fiscal year, the optional provision still offers flexibility to the Financial Institutions to determine the account value or balance and the related payment amounts based on the specificities of different types of Financial Accounts, in particular for those Financial Accounts where it may not be easy or possible to identify the account value or balance and related payment amounts at the end of a calendar year.

69. CRS Commentary on Section I(A)(4) through (7), paragraph 15.

How can the option be implemented?

Where a jurisdiction introduces this option, their administrative compliance framework and relevant verification activities should take this into consideration to ensure that it has been only applied by Financial Institutions in line with the requirements and that it has not been used to manipulate year-end amounts and circumvent the reporting requirements.

6.3.5. Phasing in the requirement to report gross proceeds

The option to report gross proceeds in a later year was introduced to allow Reporting Financial Institutions to have additional time to implement systems and procedures to capture gross proceeds for the sale or redemption of Financial Assets.

While the CRS and its Commentary foresee the possibility of allowing jurisdictions to phase in the requirement to report gross proceeds from the sale or redemption of Financial Assets paid or credited to the accounts during the calendar year or other appropriate reporting period, this approach is not facilitated under the CRS MCAA. It is therefore not considered further within this toolkit.

6.3.6. Requirement to file nil returns

What is it and what does it allow for?

Although all Reporting Financial Institutions must carry out due diligence, the Standard only requires them to report information in respect of any Reportable Accounts that they maintain (which the due diligence identifies). In practice, all such Reportable Accounts are reported to the tax authority through the filing of a return (often in the form of an electronic file).

Jurisdictions can opt to also require Reporting Financial Institutions with no Reportable Accounts to still file a return for the purposes of confirming that they did not have any Reportable Accounts and related information to report.

When can this provision help jurisdictions?

The option of requiring the filing of nil return has been widely adopted by jurisdictions as it has been considered a helpful tool within a jurisdiction's administrative compliance framework to:

- more easily identify all Reporting Financial Institutions, particularly those that are not regulated by a financial supervisory authority or similar
- better monitor their compliance with their reporting obligation, including by providing them with an opportunity to efficiently state why they have not reported (rather than being asked through follow-up enquiries).

Identifying all Reporting Financial Institutions is a necessary activity in ensuring that all Financial Institutions have fulfilled their obligations. Nil reporting obligations serve as helpful and complementary tools alongside a jurisdiction's other compliance activities.

How can the option be implemented?

The model rules, both the copy out (available on request) and reference (Annex C of the toolkit) methods, include this option.

Jurisdictions adopting a nil filing requirement should reflect how they will collect nil returns from their Financial Institutions. This can be done by:

- adapting their AEOI Portal to receive nil returns
- introducing a tailored means of allowing Reporting Financial Institutions to notify the competent authority that they have no Reportable Accounts for each reporting period. For this, the jurisdiction could create a paper or electronic nil return form which includes an attestation by the Reporting Financial Institution confirming that it has carried out the CRS due diligence requirements set out in law and that it identified no Reportable Accounts for that reporting period.

Verification activities should be carried out to determine the correctness of the nil report, namely that the Reporting Financial Institution carried out the necessary due diligence obligations correctly and that there were no Reportable Accounts.

6.3.7. Use of third party service providers by Financial Institutions

What is it and what does it allow for?

Jurisdictions may allow Reporting Financial Institutions

to use service providers to fulfil the reporting and due diligence obligations on their behalf. This includes allowing Reporting Financial Institutions to rely on the due diligence procedures performed by third party service providers.

Under this option, the Reporting Financial Institutions must still meet the CRS requirements set out under domestic law, including obligations under domestic law on confidentiality and data protection. The Reporting Financial Institutions must remain responsible for the fulfilment of their CRS obligations (the actions of the service providers are attributed to the Reporting Financial Institutions). The service providers may be resident in the same or in a different jurisdiction as the Reporting Financial Institution, subject to any other relevant domestic law. However, the time and manner of the reporting and due diligence obligations remain the same as if they were still being fulfilled by the Reporting Financial Institution.

When can this provision help jurisdictions?

This option has been widely adopted by jurisdictions as it offers conveniences and flexibility to the Reporting Financial Institutions when implementing procedures to comply with their CRS obligations. Certain Reporting Financial Institutions may for example find it more practicable to have a third party obtain valid self-certifications on account opening or where the third party already has a direct relationship with the Account Holder, such as a fund managed by the fund manager or a trust that is managed and administered by its trustee.

How can the option be implemented?

The model rules, both the copy out (available on request) and reference (Annex C of the toolkit) methods, include this option.

Where a jurisdiction introduces this option for its Reporting Financial Institutions, they will have to adapt their verification activities undertaken as part of their administrative compliance framework accordingly. This would include ensuring that records of the steps undertaken and any evidence relied upon for the performance of the due diligence and reporting procedures are maintained by the Financial Institution or that the Financial Institution can obtain those records when required, including when requested by the tax authority (CRS, Section IX(A)(2)).

6.3.8. New Account due diligence procedures for Preexisting Accounts

What is it and what does it allow for?

Jurisdictions may allow Reporting Financial Institutions to apply the due diligence procedures for New Accounts to Preexisting Accounts. Customers opening New Accounts are required to provide additional information including the self-certifications to Reporting Financial Institutions to determine where they are resident for tax purposes, whilst for Preexisting Accounts, Reporting Financial Institutions can generally rely on the information they hold on file. Therefore, allowing the due diligence procedures for New Accounts to be applied to Preexisting Accounts means that Reporting Financial Institutions could elect to collect additional information including self-certifications from all Preexisting Accounts, instead of applying the related due diligence procedures for Preexisting Accounts.

Jurisdictions offering this option may also permit Reporting Financial Institutions to apply the option for all relevant Preexisting Accounts or, separately, for any clearly identified group of such accounts, such as by line of business or the location where the account is maintained (Commentary on Section II(E), paragraphs 8 and 9).

Even though Reporting Financial Institutions may elect to apply New Account due diligence procedures to Preexisting Accounts under this option, the rules otherwise applicable to Preexisting Accounts continue to apply. This includes the following relieving rules that apply to Preexisting Accounts:

- The exception rules applicable to Preexisting Accounts where the TIN or date of birth is not required to be reported under certain conditions (CRS, Section I(C)).
- The exemption rules on due diligence for Preexisting Individual Accounts that are Cash Value Insurance Contracts and Annuity Contracts if the Reporting Financial Institution is effectively prevented by law from selling such contracts to residents from Reportable Jurisdictions (CRS, Section III(A)).
- The exemption rules for Preexisting Entity Accounts with the account balance or value (after aggregation) of USD 250 000 or less at the date set to determine Preexisting Accounts or at the end of any subsequent calendar year, and the Reporting Financial Institutions wish to apply the threshold (if it is permitted by the domestic CRS rules) (CRS, Section V(A)).

- The reporting of a single residence for a Preexisting Individual Account is sufficient to satisfy the reporting requirements regarding the information to be reported, to be consistent with the residence address test rules for Preexisting Lower Value Accounts (CRS, Section III(B)(1)).

When can this provision help jurisdictions?

Allowing the due diligence procedures for New Accounts to be used for Preexisting Accounts is an option that has been widely offered by jurisdictions, as it gives the Reporting Financial Institutions flexibility in conducting the due diligence procedures for Preexisting Accounts, based on their own specific business needs. For example, a Reporting Financial Institution that does not maintain many Financial Accounts might find it easier to obtain self-certifications in respect of Preexisting Accounts. The Reporting Financial Institution will however still have to carry out the Preexisting Account due diligence requirements on those Financial Accounts where it has been unable to obtain a valid self-certification.

Obtaining self-certifications in respect of Preexisting Accounts is considered as a more effective route to establishing where Account Holders and Controlling Persons are resident for tax purposes. Adopting this optional provision can therefore also help to increase the quality and accuracy of the information reported by the Reporting Financial Institutions and then exchanged with partner jurisdictions.

How can the option be implemented?

The model rules, both the copy out (available on request) and reference (Annex C of the toolkit) methods, include this option.

Where a jurisdiction introduces this option for its Reporting Financial Institutions, they will have to adapt their verification activities undertaken as part of their administrative compliance framework accordingly. This would include ensuring that records of the steps undertaken and any evidence relied upon for the performance of the due diligence and reporting procedures are maintained by the Financial Institution or that the Financial Institution can obtain those records when required, including when requested by the tax authority (CRS, Section IX(A)(2)).

6.3.9. High Value Account due diligence procedures for Lower Value Accounts

What is it and what does it allow for?

Jurisdictions may allow Reporting Financial Institutions to apply the due diligence procedures for High Value Accounts to Lower Value Accounts. This would mean that the enhanced due diligence procedures as required by the CRS for High Value Accounts can be equally applied to Lower Value Accounts, including the Paper Record Search and the Relationship Manager Inquiry for Actual Knowledge.

Under the CRS, if a Preexisting Individual Account is not a High Value Account at the date set to determine Preexisting Accounts, but it later becomes a High Value Account as of the last day of a subsequent calendar year (i.e. the account balance or value exceeds USD 1 million), the Reporting Financial Institution must apply the due diligence procedures for the High Value Accounts (CRS, Section III(C)(6)). Under this default approach, the Reporting Financial Institutions would have to ensure such accounts are identified in order to follow up on them with the necessary due diligence activities. If the Reporting Financial Institutions instead apply the due diligence procedures for High Value Accounts to Lower Value Accounts, this ongoing need to identify these accounts can be partly or fully alleviated.

Jurisdictions offering this option may permit Reporting Financial Institutions to apply the option for all relevant Preexisting Accounts or, separately, for any clearly identified group of such accounts, such as by line of business or the location where the account is maintained (Commentary on Section II(E), paragraphs 8 and 9).

When can this provision help jurisdictions?

Allowing the due diligence procedures for High Value Accounts to Lower Value Accounts is an option that has been widely adopted by jurisdictions, as it gives the Reporting Financial Institutions flexibility to apply the due diligence procedures for Preexisting Accounts based on their own business needs. For example, a Reporting Financial Institution that does not maintain many Financial Accounts might be preferable to apply the same due diligence steps on all accounts, because this allows it to forego checking annually whether any of its Lower Value Accounts become High Value Accounts.

How can the option be implemented?

The model rules, both the copy out (available on request) and reference (Annex C of the toolkit) methods, include this option.

Where a jurisdiction introduces this option for its Reporting Financial Institutions, they will have to adapt their verification activities undertaken as part of their administrative compliance framework accordingly. This would include ensuring that records of the steps undertaken and any evidence relied upon for the performance of the due diligence and reporting procedures are maintained by the Financial Institution or that the Financial Institution can obtain those records when required, including when requested by the tax authority (CRS, Section IX(A)(2)).

6.3.10. Residence address test for Lower Value Accounts

What is it and what does it allow for?

Jurisdictions may permit their Financial Institutions to apply a simplified approach of relying on the Account Holder's residence address to determine their residence for tax purposes, as well as whether the account is a Reportable Account. Where this option is provided for in legislation, the residence address test exists as an alternative, and not a replacement, to the default indicia based approach of establishing residence. If the residence address test cannot be applied, the Financial Institution must perform the electronic indicia search.

Financial Institutions may only apply the residence address test instead of the default approach on accounts where all requirements set out in paragraphs 7-19 of the Commentary on Section III(B)(1) are met, including that:

- The account is a Preexisting Lower Value Account (account balance does not exceed USD 1 million).
- The account is held by an individual Account Holder.
- The Financial Institution has in its records a residence address for the individual Account Holder and the address held is current and based on Documentary Evidence.

When can this provision help jurisdictions?

The residence address test is an option that has been widely adopted by jurisdictions as it is considered a materially simplified due diligence approach for Financial Institutions. Financial Institutions choosing to apply the residence address test may not be able to do so for all cases, and this does not alleviate them of other due diligence requirements applicable to the same accounts, such as where there is a change of circumstances. Nevertheless, the residence address test can substantially alleviate the resource required by Financial Institutions to carry out due diligence across their accounts, particularly if a large proportion of these are low value and held by individuals.

How can the option be implemented?

The model rules, both the copy out (available on request) and reference (Annex C of the toolkit) methods, include this option.

Where a jurisdiction introduces this option for Financial Institutions, they will have to adapt their verification activities undertaken as part of their administrative compliance framework accordingly, so as to ensure that all Financial Institutions which have chosen to apply the residence address test only do so when all requirements set out in the CRS and its Commentary have been met.

6.3.11. Exclusions for Preexisting Entity Accounts of USD 250 000 or less

What is it and what does it allow for?

A jurisdiction may permit their Reporting Financial Institutions to exclude Preexisting Entity Accounts from the due diligence procedures if they have an aggregate account balance or value of USD 250 000 or less as of a specified date. This date will typically be the same date chosen to define Preexisting Account.

Where this option has been permitted by the jurisdiction the Reporting Financial Institution may elect to apply it either with respect to all Preexisting Entity Accounts or, separately, with respect to any clearly identified group of such accounts. These accounts will only remain exempt so long as their aggregate account balance or value does not exceed USD 250 000 at the end of a subsequent calendar year. If this happens, the due diligence procedures for Preexisting Entity Accounts must be applied.

When can this provision help jurisdictions?

This exclusion is an option that has been widely adopted by jurisdictions. It is provided to reduce the compliance burden on Reporting Financial Institutions, considering

that the due diligence procedures for accounts held by Entities are more complex than those for accounts held by individuals.

How can the option be implemented?

The model rules, both the copy out (available on request) and reference (Annex C of the toolkit) methods, include this option.

Where a jurisdiction introduces this option for Reporting Financial Institutions, they will have to adapt their verification activities undertaken as part of their administrative compliance framework accordingly. They should ensure that all Reporting Financial Institutions that have applied this option have only done so in line with the requirements and that they have adequate procedures in place to annually identify any Entity accounts whose aggregate balance exceeds USD 250 000 and subsequently carry out the necessary due diligence requirements.

6.3.12. Alternative documentation procedure for certain Group Insurance Contracts or Annuity Contracts

What is it and what does it allow for?

Reporting Financial Institutions are able to treat certain Cash Value Insurance Contracts or Annuity Contracts as accounts that are not Reportable Accounts (CRS, Section IX(A)(2)). This is allowed when the beneficiaries (other than the owner) of a death benefit is not the direct client of the Reporting Financial Institution and the information collected from this person might not be sufficient to determine their status as a Reportable Person. However, if the Reporting Financial Institution has actual knowledge or reason to know that the beneficiary of the contract is a Reportable Person, then the account becomes a Reportable Account.

Another common example of a situation where the Reporting Financial Institution does not have direct contact with the beneficiaries of an account is where Group Cash Value Insurance Contracts or Group Annuity Contracts are issued to an employer or association in the benefit of its employees or members. Jurisdictions are able to permit their Reporting Financial Institutions to also treat these accounts as not Reportable Accounts until the date on which an amount is payable to the employee/certificate holder or beneficiary. This approach recognises that the Financial Institution does not have a direct relationship with the employee/certificate holder at the inception of the contract and may not be able to obtain documentation regarding their residence.

This option must be reflected in the domestic legal framework and it may only be permitted for use by Reporting Financial Institutions where the all requirements are met (Commentary on Section VII(B), paragraph 13):

- The Group Cash Value Insurance Contract or a Group Annuity Contract is issued to an employer or association. This means that the client of the Reporting Financial Institution is the employer and not the employees/beneficiaries.
- The account covers 25 or more employees. For accounts with less than 25 beneficiaries, the Reporting Financial Institution will have to conduct the regular due diligence procedures to identify all beneficiaries and report the account if any of them is found to be a Reportable Person.
- The employee / certificate holder is entitled to receive a contract value related to their interest. This means that the certificate holder, and not the employer/ association, has the right to receive the amount deposited in their name and any related interest on it.
- The employee / certificate holder is entitled to name beneficiaries for the benefit to be payable upon their death. This means that the right to the interest in the account is not perishable upon the death of the employee/certificate holder but it can be transferred to the named beneficiaries.
- The aggregate amount payable to any employee/ certificate holder or beneficiary does not exceed USD 1 million. This means that when any particular certificate holder or named beneficiary is entitled to more than USD 1 million from the account, the Reporting Financial Institution will have to conduct the regular due diligence procedures and report the account if the certificate holder or beneficiary is found to be a Reportable Person.

When can this provision help jurisdictions?

Jurisdictions may wish to include this option to reduce the due diligence burden on Financial Institutions that hold Group Cash Value Insurance Contracts or a Group Annuity Contracts. When all the conditions are met, the

Reporting Financial Institution would not be required to follow regular due diligence procedures to identify whether each employee/certificate holder or beneficiary is a Reportable Person upon account opening or upon the addition of each new employee/certificate holder or beneficiary to the account.

How can the option be implemented?

To provide this option, the implementing jurisdiction may include or reference in their domestic legislation the language proposed in paragraph 13 of the Commentary on Section VII.

> *A Reporting Financial Institution may treat a Financial Account that is a member's interest in a Group Cash Value Insurance Contract or Group Annuity Contract as a Financial Account that is not a Reportable Account until the date on which an amount is payable to the employee/certificate holder or beneficiary, if the Financial Account that is a member's interest in a Group Cash Value Insurance Contract or Group Annuity Contract meets the following requirements:*
>
> *a) the Group Cash Value Insurance Contract or Group Annuity Contract is issued to an employer and covers twenty-five or more employee/certificate holders;*
>
> *b) the employee/certificate holders are entitled to receive any contract value related to their interests and to name beneficiaries for the benefit payable upon the employee's death; and*
>
> *c) the aggregate amount payable to any employee/certificate holder or beneficiary does not exceed USD 1 000 000.*
>
> *The term "Group Cash Value Insurance Contract" means a Cash Value Insurance Contract that (i) provides coverage on individuals who are affiliated through an employer, trade association, labour union, or other association or group; and (ii) charges a premium for each member of the group (or member of a class within the group) that is determined without regard to the individual health characteristics other than age, gender, and smoking habits of the member (or class of members) of the group. The term "Group Annuity Contract" means an Annuity Contract under which the obligees are individuals who are affiliated through an employer, trade association, labour union, or other association or group.*

The model rules, both the copy out (available on request) and reference (Annex C of the toolkit) methods, include this option.

It is important to note that upon the date on which an amount is payable, the Reporting Financial Institution will have the obligation to follow due diligence procedures to determine if the beneficiary is a reportable person and report the account accordingly. Therefore, where a jurisdiction introduces this option for its Reporting Financial Institutions, they will have to adapt their verification activities undertaken as part of their administrative compliance framework accordingly. They should ensure that any Reporting Financial Institutions applying this option only does so when all the aforementioned requirements are met and that they have the required policies and procedures and implement the due diligence procedures at the appropriate times.

6.3.13. Allowing existing standardised industry coding systems in due diligence procedures

What is it and what does it allow for?

Jurisdictions may permit their Reporting Financial Institutions to use existing standardised industry coding systems as Documentary Evidence when carrying out due diligence on Preexisting Entity Accounts. Where the jurisdiction permits this option, a Reporting Financial Institution may only apply this to Financial Accounts where the following conditions are met:

- Any classification based on a standardised industry coding system was recorded consistent with its normal business practices for purposes of AML/KYC Procedures or other regulatory purposes.
- This was implemented prior to the date used to classify the Financial Account as a Preexisting Account.
- It has no reason to know that the classification is incorrect or unreliable.

A jurisdiction may choose to give clarity to its Reporting Financial Institutions by specifying that particular industry coding systems may be used for this purpose, or should not be used. The jurisdiction can do this by way of guidance.

When can this provision help jurisdictions?

This is an option that has been widely adopted by jurisdictions. It is provided to reduce the due diligence burden on Financial Institutions by building upon existing business practices.

How can the option be implemented?

The model rules, both the copy out (available on request) and reference (Annex C of the toolkit) methods, include this option.

Where a jurisdiction introduces this option for Reporting Financial Institutions, they will have to adapt their verification activities undertaken as part of their administrative compliance framework accordingly. They should ensure that all Reporting Financial Institutions that have applied this option have only done so on Financial Accounts where all of the aforementioned requirements are met as well as any further requirements set out by the jurisdiction in terms of acceptable industry coding systems.

6.3.14. Currency translation

What is it and what does it allow for?

The CRS provides for several thresholds established in USD to determine specific due diligence rules to be applied to accounts. For example, the rules on reviewing Preexisting Accounts with a balance of USD 1 million or under differ from High Value Accounts whose balances exceed that amount. The default approach under the CRS therefore requires Financial Institutions that hold accounts in other currencies would apply the corresponding exchange rates.

Jurisdictions may choose to permit their Reporting Financial Institutions to apply thresholds in USD or to apply the threshold with their equivalent amounts in other currencies. Implementing jurisdictions are expected to use amounts that are equivalent to the USD amounts in the CRS, but when translating to other currencies, the amounts do not need to be exact and approximate equivalents are sufficient.

When drafting its domestic legislation implementing jurisdictions can opt to determine thresholds:

- in the domestic currency: the amount can be an approximate equivalent to the USD amounts required by the CRS.
- in USD amounts along with equivalents in other currencies: this would allow Financial Institutions that operate in several jurisdictions to apply the thresholds in the same currency as the accounts are denominated.

When can this provision help jurisdictions?

Introducing the option on Reporting Financial Institutions to apply thresholds in their USD equivalent has been widely adopted by jurisdictions.[70] Jurisdictions should consider the composition of their Financial Institution population. If it includes a notable proportion of transnational Financial Institutions, allowing the option to determine thresholds from several currencies might facilitate the due diligence and reporting procedures. This is particularly the case where Reporting Financial Institutions regularly offer products in more than one currency. The option to determine thresholds from several currencies will allow Financial Institutions that offer products in several currencies to apply the thresholds most relevant to the account.

How can the option be implemented?

The model rules, both the copy out (available on request) and reference (Annex C of the toolkit) methods, include the option to allow Reporting Financial Institutions to apply the thresholds in US dollars or equivalents in other currencies.

Where a jurisdiction introduces this option for Reporting Financial Institutions, they will have to adapt their verification activities undertaken as part of their administrative compliance framework accordingly to ensure that Reporting Financial Institutions only use equivalent amounts in the respective currency and that this is not subject to abuse intended to circumvent due diligence or reporting.

The reference method refers to the CRS and its Commentary where USD amounts are included. If the jurisdiction wished to instead require domestic currency amounts to be used, it would have to amend the rules accordingly. Alternatively, the jurisdiction could set out what it considers to be USD equivalent amounts in its own currency in guidance for its Reporting Financial Institutions.

70. Introducing the thresholds in non-USD amounts comes with an expectation that the jurisdiction will monitor exchange rate changes over time and if the thresholds become materially higher than the USD equivalent, the non-USD thresholds must be adjusted.

6.3.15. Currency election

The information reported must always identify the currency in which each amount is denominated. Although it is not an optional provision that has to be introduced into legislation, jurisdictions should be aware that, regardless of the currency used in the domestic legislation to set amounts for thresholds in the due diligence rules, Reporting Financial Institutions must report the balance of the account in the currency that the Reportable Account is denominated in.

If an account is denominated in more than one currency, then the Financial Institution may decide in which of those currencies to report the account, taking care to always identify which currency has been used (Commentary to Section I(B), paragraph 23).

6.3.16. Expanded definition of Preexisting Account

What is it and what does it allow for?

The CRS classifies accounts as "Preexisting Accounts" or "New Accounts" depending of the date of account opening. The implementing jurisdiction will determine this cut-off date in line with its own implementation schedule (see Subsection 6.2.1 of this toolkit). These dates will be set out in their respective definitions in the domestic legislation (CRS, Section VIII(C) (9) and (10)).

Jurisdictions have the option to expand the definition of Preexisting Accounts to include accounts opened by preexisting clients after the cut-off date when certain conditions are met (Commentary to Section VIII(C), paragraph 82):

- The account holder has a Preexisting Account with the Financial Institution (or a Related Entity within the same jurisdiction).
- The Financial Institution treats both accounts as a single account for the purposes of satisfying standards of knowledge requirements (set out in CRS, Section VII(A)) and to determine the balance or value of the accounts when applying thresholds.
- The Financial Institution is permitted to rely on the AML/KYC procedures performed on the earlier account for the later account.
- Except for the CRS due diligence, the opening of the account does not require the provision of new, additional or amended client information.

Where a Financial Institution requests or otherwise obtains any new, additional or amended client information, whether related to AML/KYC requirements or not, the conditions are not met and the account should be treated as a New Account.

When can this provision help jurisdictions?

This option will mean that Financial Institutions can rely on due diligence of Preexisting Accounts in cases where they open accounts for existing clients without requiring additional information or signatures.

Jurisdictions may wish to include this option to reduce the due diligence burden on all existing Financial Institutions with client relationships in place. When all conditions are met, the Reporting Financial Institution would not be required to follow the regular due diligence procedures for New Accounts to identify if the Account Holder or Controlling Person is a Reportable Person upon account opening.

How can the option be implemented?

To provide this option, the implementing jurisdiction must replace Section VIII(C)(9) of the CRS with the language provided in paragraph 82 of the Commentary on Section VIII(C)(9).

> *9. The term "Preexisting Account" means:*
>
> *a) a Financial Account maintained by a Reporting Financial Institution as of [xx/xx/xxxx].*
>
> *b) any Financial Account of an Account Holder, regardless of the date such Financial Account was opened, if:*
>
> *i) the Account Holder also holds with the Reporting Financial Institution (or with a Related Entity within the same jurisdiction as the Reporting Financial Institution) a Financial Account that is a Preexisting Account under subparagraph C(9)(a);*

ii) the Reporting Financial Institution (and, as applicable, the Related Entity within the same jurisdiction as the Reporting Financial Institution) treats both of the aforementioned Financial Accounts, and any other Financial Accounts of the Account Holder that are treated as Preexisting Accounts under this subparagraph C(9)(b), as a single Financial Account for purposes of satisfying the standards of knowledge requirements set forth in paragraph A of Section VII, and for purposes of determining the balance or value of any of the Financial Accounts when applying any of the account thresholds;

iii) with respect to a Financial Account that is subject to AML/KYC Procedures, the Reporting Financial Institution is permitted to satisfy such AML/KYC Procedures for the Financial Account by relying upon the AML/KYC Procedures performed for the Preexisting Account described in subparagraph C(9)(a); and

iv) the opening of the Financial Account does not require the provision of new, additional or amended customer information by the Account Holder other than for purposes of the Common Reporting Standard.

The model rules, both the copy out (available on request) and reference (Annex C of the toolkit) methods, include this option.

Where a jurisdiction expands the definition of Preexisting Account, they will have to adapt their verification activities undertaken as part of their administrative compliance framework accordingly to ensure that Reporting Financial Institutions only treat new accounts as Preexisting Accounts where all of the requirements are met.

6.3.17. Expanded definition of Related Entity

What is it and what does it allow for?

The CRS defines a "Related Entity" of another Entity as one where either Entity controls the other Entity, or the two Entities are under common control (CRS, Section VIII(E)(4)). For this purpose control includes direct or indirect ownership of more than 50% of the vote and value in an Entity.

Under this definition, an investment fund would not normally qualify as a Related Entity of another fund under the same management. Therefore, when jurisdictions provide the expanded definition of Preexisting Accounts described (see Subsection 6.3.16 of this toolkit), fund managers with due diligence obligations would not be able to use this option for their existing clients that open accounts with different funds under their same management.

Jurisdictions have the option to expand the definition of Related Entity to allow Investment Entities to apply the expanded definition of Preexisting Accounts when conducting customer due diligence. The expanded definition of Related Entity will include another Entity when all of the following requirements are met:

- both Entities are Investment Entities described in Section VIII(A)(6)(b) of the CRS
- both Entities are under common management
- the management fulfils the due diligence obligations of both Entities.

When can this provision help jurisdictions?

Jurisdictions that consider expanding the definition of Preexisting Accounts should also consider this expanded definition of Related Entity to allow Investment Entities to rely on Preexisting Accounts due diligence procedures for accounts opened after the cut-off date for New Accounts.

How can the option be implemented?

To provide this option, the implementing jurisdiction must replace Section VIII(E)(4) of the CRS with the language provided paragraph 82 of the Commentary on Section VIII(C)(9):

4. An Entity is a "Related Entity" of another Entity if (a) either Entity controls the other Entity; (b) the two Entities are under common control; or (c) the two Entities are Investment Entities described in subparagraph A(6)(b), are under common management, and such management fulfils the due diligence obligations of such Investment Entities. For this purpose control includes direct or indirect ownership of more than 50% of the vote and value in an Entity.

The model rules, both the copy out (available on request) and reference (Annex C of the toolkit) methods, include this option.

6.3.18. Grandfathering of bearer shares issued by Exempt Collective Investment Vehicle

What is it and what does it allow for?

The CRS provides for a category of Non-Reporting Financial Institution described as "Exempt Collective Investment Vehicle". In essence, a Collective Investment Vehicle (CIV) is eligible if it is regulated and all of the interests in it are held by or through persons who are not Reportable Persons and, in the case of a Passive NFE holding an interest, none of its Controlling Persons are Reportable Persons.

Jurisdictions could, if they wish, simply define an Exempt Collective Investment Vehicle using only the first paragraph of its definition in the CRS. However, there is optional further text available to jurisdictions wishing to offer this exclusion to CIVs that have issued bearer shares. This concession is subject to conditions (CRS, Section VIII(B)(9)), in particular that the CIV:

i. does not issue any physical shares in bearer form after a specified date, which should be no later than the commencement date for the CRS in the jurisdiction

ii. retires any existing bearer shares upon surrender

iii. carries out the CRS due diligence when such shares are presented for redemption or other payment and reports any information accordingly

iv. has policies and procedures to redeem or immobilise such shares as soon as possible and in any event by a specified date, which may be later than the first date indicated in (i) above, but delayed by no more than what would be a reasonable time for CIVs to put in order existing bearer shares.

When can this provision help jurisdictions?

In practice, CIVs that are Investment Entities and whose interests are held by or through non-Reportable Persons would generally not having any reporting obligations irrespective of whether it qualifies as an Exempt Collective Investment Vehicle. However, such qualification may be relevant to other obligations on the Investment Entity such as any nil filing return obligations in the jurisdiction. By having this optional provision in place, jurisdictions will also remove such obligations from any CIVs that meet the requirements even if they have issue bearer shares.

How can this option be implemented?

The model rules, both the copy out (available on request) and reference (Annex C of the toolkit) methods, include this option which is by default included in the CRS. In practice, jurisdictions may choose to amend their domestic legislation or the model rules to remove the possibility of the definition of Exempt Collective Investment Vehicles extending to CIVs which have in the past issued bearer shares.

6.3.19. Controlling Persons of a trust

What is it and what does it allow for?

When conducting due diligence for CRS purposes, the settlor(s), trustee(s), protector(s) and beneficiary(ies) are always considered Controlling Persons in addition to any natural person exercising ultimate effective control of a trust. Beneficiaries of a trust can be persons with the right to receive a mandatory benefit or persons that may receive a discretionary benefit (or distribution) at some point.

Where trusts are Financial Institutions, the CRS determines that persons with a right to receive a discretionary benefit will only be treated as a beneficiary in the relevant reporting period when the person receives a distribution (Commentary on Section VIII(C)(4), paragraph 70).

When implementing the CRS, jurisdictions may permit Reporting Financial Institutions to align the scope of beneficiaries of a trust who are treated as Controlling Persons with the scope set out for beneficiaries of trusts which are Financial Institutions. In practice, this means that the discretionary beneficiaries of a trust would only be considered a Controlling Person in the reporting periods when a distribution is received. Therefore, Reporting Financial Institutions would only need to report discretionary beneficiaries in the year that these beneficiaries receive a distribution from the trust.

When can this provision help jurisdictions?

When implementing this option, Financial Institutions will not have to identify and report discretionary beneficiaries of a trust until it is certain that they will receive a distribution. When this option is not implemented, Financial Institutions will have reporting obligations for potential (but not certain) beneficiaries of a trust even without the distribution ever being realised. This information is not as relevant for the receiving jurisdictions as the taxpayer has not received or is not certain to receive any income.

The due diligence obligations are not necessarily reduced. Financial Institutions, in all cases, have the obligation to obtain sufficient information to establish the identity of the beneficiaries. When the implementing jurisdiction applies this option, Financial Institutions must also ensure there are controls in place to identify when a distribution is made.

Nevertheless, this option has been widely adopted by jurisdictions which recognise trusts or other similar legal arrangements as it can ensures exchange partners will receive the information when most relevant.

How can this option be implemented?

This option can be implemented either by referencing paragraph 70 of the Commentary on of the Commentary on Section VIII(C(4) of the CRS in the definition of Controlling Persons or adding the following paragraph to the definition of Controlling Persons:

> *The beneficiary(ies) of a trust is a person with the right to receive, directly or indirectly (for example, through a nominee), a mandatory distribution or may receive, directly or indirectly, a discretionary distribution from the trust. For these purposes, a beneficiary who may receive a discretionary distribution from the trust only will be treated as a beneficiary of a trust if such person receives a distribution in the calendar year or other appropriate reporting period (i.e. either the distribution has been paid or made payable). The same is applicable with respect to the treatment of a Reportable Person as a beneficiary of a legal arrangement that is equivalent or similar to a trust, or foundation.*

The model rules, both the copy out (available on request) and reference (Annex C of the toolkit) methods, include this option. Where a jurisdiction introduces this option for Reporting Financial Institutions, they will have to adapt their verification activities undertaken as part of their administrative compliance framework accordingly to ensure that Reporting Financial Institutions that apply this approach have adequate processes in place to ensure that information is reported whenever distributions are made to discretionary beneficiaries.

6.3.20. The wider approach and similar options

What is it and what does it allow for?

The default due diligence procedures in the CRS (in particular Preexisting Account procedures) are designed to identify Account Holders and Controlling Persons that would be resident for tax purposes in any jurisdiction included in the domestic list of Reportable Jurisdictions at the time the due diligence procedures are carried out or in case of a change of circumstances. However, jurisdictions may opt to go beyond this requirement and adopt what has been termed as the "wider approach". This approach refers to extending the due diligence procedures to require Reporting Financial Institutions to identify and collect information on all Account Holders and Controlling Persons tax resident in any other jurisdiction, not only those listed as Reporting Jurisdictions.

The wider approach does not require the Reporting Financial Institutions to report this additional information (i.e. concerning persons tax resident in the jurisdictions not listed as Reportable Jurisdictions). In practice, this means that the information is only held by the Financial Institutions themselves. It is nevertheless possible to take this approach further and require Financial Institutions to identify and report upon all Account Holders and Controlling Persons resident for tax purposes in another jurisdiction. This has been termed as the "widest approach". Under the widest approach the information is only reported to the tax administration but not automatically exchanged, as there would be no obligation or legal basis to do so.

Finally, a jurisdiction may take the opportunity of the implementation of the CRS to increase transparency on the Financial Accounts held domestically by its tax residents and introduce a domestic reporting regime by way of requiring Financial Institutions to also report CRS data on its own tax residents.

When can this provision help jurisdictions?

The wider approach is one of the most commonly adopted provisions (adopted by approximately 80% of the CRS adopters). Jurisdictions have done so on the basis of potential efficiencies that can be gained, at both the level of Reporting Financial Institutions and the implementing jurisdiction.

Not adopting the wider approach would mean that Reporting Financial Institutions could have to revisit due diligence procedures across their Financial Accounts each time new jurisdictions are added to the domestic list of Reportable Jurisdictions. Due diligence steps which can be particularly time consuming, such as the paper record search would have to be carried out across all accounts again to identify whether they have become reportable.

The wider approach will instead mean that Reporting Financial Institutions will already have completed the due diligence by the time the list of Reportable Jurisdictions is expanded, so they will already know whether they have any new Reportable Accounts.

While most of the efficiencies will have already been gained by the implementation of the wider approach, the widest approach could also create further efficiencies at the level of the Reporting Financial Institutions as it would require them to carry out less sorting of the information collected (i.e. the Reporting Financial Institutions would not have to extract the information which would not be exchanged to another jurisdiction for any particular year).

Where jurisdictions do not have a domestic reporting regime in place which requires reporting on Financial Accounts held by their own tax residents, expanding the scope of reportable information to all Account Holders can provide tax administrations with a valuable source of information to verify their own taxpayers' compliance.

How can the option be implemented?

The model rules, both the copy out (available on request) and reference (Annex C of the toolkit) methods, include the option of the wider approach through the definition of Reportable Jurisdiction.

If a jurisdiction considers implementing the widest approach or to take advantage of the implementation of the CRS to introduce a domestic reporting, the model rules would have to be adjusted accordingly.

7. Ensuring effective implementation

7.1. ADMINISTRATIVE COMPLIANCE FRAMEWORK

Jurisdictions should ensure that in practice Reporting Financial Institutions correctly implement the due diligence and reporting procedures, which includes a requirement for jurisdictions to have in place an administrative framework to ensure the effective implementation of the CRS (ToR, CR 1 Effectiveness in practice). The administrative compliance framework should be based on a strategy that enables the implementing jurisdictions to facilitate voluntary compliance and to take appropriate enforcement measures when deficiencies are identified.

This section of the toolkit highlights areas to consider when planning for effective implementation of the Standard.

The Forum on Tax Administration (FTA) has produced more specific guidance on ensuring compliance by Financial Institutions with their CRS obligations.[71]

7.1.1. Compliance strategy

In order to ensure Financial Institutions comply with the requirements set out in the Standard, the implementing jurisdiction will need to develop a strategy. This strategy not only concerns putting in place all the necessary steps and measures needed as part of an effective administrative compliance framework, but it should also act as the basis for ensuring that the correct risks are identified and that resources are allocated accordingly. The key elements to incorporate in the strategy include:

- ensuring that the authority(ies) responsible for supervising the implementation of the Standard have the necessary powers to enforce the requirements
- ensuring that the authority(ies) responsible for supervising the implementation of the Standard identify and allocate the resources (financial, human, technical) needed to ensure an effective implementation of the Standard
- carrying out a risk assessment to understand compliance risks, including jurisdiction-specific risks, and using that information to design strategies to address these risks

71. OECD (2020), Automatic Exchange of Information: Guide on Promoting and Assessing Compliance by Financial Institutions, op. cit.

- developing a compliance plan, covering all of the key areas set out in the ToR, with activities to be carried out in a staged approach with clear timelines
- implementing strategies to encourage voluntary compliance
- developing and implementing the procedures needed to carry out checks and verification of compliance
- putting in place enforcement mechanisms to address non-compliance
- routinely evaluating and improving the compliance plan as necessary, including refreshing the risk assessment
- following up on any feedback or notifications received from exchange partners.

The strategy should identify the various stakeholders within and outside the primary authority(ies) responsible for implementing the Standard, and allocate the respective responsibilities for ensuring compliance in practice. The strategy should be documented and monitored on a regular basis with statistics collected on the compliance activities performed and the sanctions applied.

7.1.2. Encouraging voluntary compliance

The implementation of the Standard brings a number of new challenges to Financial Institutions, as they need to understand and implement new procedures. The starting point of an effective compliance framework is to encourage Financial Institutions to voluntarily comply with the new requirements through awareness raising, education, communication and outreach activities.

Communication, education and guidance

Intensive communication and outreach activities regarding the implementation of the CRS should be regularly conducted for Financial Institutions from the date of a jurisdiction's commitment until their first deadline to report information. The objective is to ensure that Reporting Financial Institutions are aware of their obligations, including their obligation to review their Financial Accounts and identify Reportable Accounts, and then to report accurate information to the tax authority in a timely manner. The communication and outreach activities can be conducted through various channels:

- Regular meetings with the representatives of Financial Institutions, such as financial industry associations (e.g. bankers' association, insurance association, trust and company service provider association), to discuss legal and technical issues regarding implementation of the Standard.
- Periodic bulletins and/or industry briefings on all upcoming obligations, including to address cross cutting issues within the industry. The content of each bulletin and briefing can follow the reporting cycle acting as a timely reminder of the steps they need to focus on.
- E-learning modules to provide guidance to Financial Institutions (e.g. introduction to the CRS, criteria to determine Reporting Financial Institution status, due diligence requirements).
- Workshops, seminars or webinars which cover practical implementation, including technical requirements, to explain challenging concepts and answer questions from the financial industry.
- FAQ section on the responsible authority(ies) website, dedicated mailboxes and phone numbers to detail with questions directly from Financial Institutions.
- Dedicated webpages where all information including detailed guidance regarding the CRS implementation can be found by Financial Institutions.
- Meetings with financial sector regulators to raise their awareness on their responsibilities in supervising the CRS obligations – if they have such a responsibility. This could take the form of interventions at their specific sector training sessions.

The communication and outreach should be planned and timed to ensure that all Financial Institutions are well informed and have any necessary guidance to fulfil their due diligence and reporting obligations.

Understanding and classifying the population of Financial Institutions

The identification of the population of Financial Institutions and how they are classified under the CRS

is needed to ensure the Standard operates effectively with all Reporting Financial Institutions aware of their status and obligations. The implementing jurisdiction responsible authority(ies) should therefore have in place a process to identify the Reporting Financial Institution population, which takes into account a wide range of relevant information sources. For example some or all of the following sources of information could be used:

- the lists of Financial Institutions that are licensed or supervised by the financial sector supervisors
- the list of Financial Institutions registered on the US Inland Revenue Service website as Foreign Financial Institutions with a GIIN, for the purposes of FATCA
- identifying potential non-regulated Financial Institutions using tax databases or commercial registers, (analysing the type of business they conduct and comparing with the lists of regulated Financial Institutions and FATCA Financial Institutions) or obtaining information from service providers and intermediaries.

The procedures taken and sources of information used should ensure the implementing jurisdiction has an up-to-date understanding of the population of Reporting Financial Institutions. It should therefore identify entities which meet the definition of Reporting Financial Institution after initial implementation of the Standard.

7.1.3. Conducting compliance audits and inspections

Organisation and resources for supervision

Jurisdictions should establish a government authority (or authorities) as responsible for supervising the Financial Institutions' compliance with their obligations in respect of the Standard. This authority should have adequate powers, procedures and resources to periodically verify this compliance.

The resources include the staffing, financial, and technical and IT resources needed to ensure compliance by Financial Institutions. The authority in charge of supervision should have a dedicated or available human resource for the CRS implementation, with compliance capabilities (e.g. CRS expertise, appropriate skills and background in risk analysis, auditing, preferably with financial industry and data management experience). The size of the human resource will depend on the number of Financial Institutions and the level of risk associated with their implementation of the Standard. Careful consideration should therefore be given on a regular basis to the adequacy of the human resource assigned to the supervision.

IT capability is also critical for the monitoring and supervision of the CRS implementation by Financial Institutions. This includes having resources available to obtain and analyse data reported for the purpose of risk assessment, identifying possible non-compliance and supporting compliance staff with their activities.

The supervisory authority(ies) should have appropriate procedures and powers to carry out their responsibilities. This includes access to Financial Institutions' records and premises (see Subsection 6.2.4 of the toolkit), access to other relevant sources of information on the activity of Financial Institutions and the ability to apply sanctions as appropriate (see Subsection 6.2.5 of the toolkit).

The implementing jurisdiction should develop and document its supervision approach and methodology. Depending on the authority in charge of supervision (e.g. the tax authority and/or the financial sector supervisors), it is likely that some supervision mechanisms are already established and can be added to or adapted. However, care needs to be taken on how the CRS supervision will work if using an existing supervision framework, particularly as not all Reporting Financial Institutions have tax obligations or are regulated for AML/CFT purposes in that jurisdiction. It should be also ensured that AEOI risks are sufficiently identified and focused on, in addition to other risks that the authorities may be responsible for monitoring.

Jurisdictions may choose to incorporate the CRS compliance activities in the general tax audits or in the inspections of the financial sector, or to conduct specific and separate compliance activities for the CRS. Regardless of the supervision model chosen, specific procedures must be developed for the CRS compliance as the checks and verifications undertaken are different.

The compliance procedures should allow the supervisory authority(ies) to ensure that:

- Financial Institutions correctly apply the definitions of Reporting Financial Institutions and Non-Reporting Financial Institutions and report information as required.

- Reporting Financial Institutions correctly apply the due diligence rules on each type of account and that they correctly report all information required.
- jurisdiction-specific Non-Reporting Financial Institutions and Excluded Accounts (if any, see Subsections 6.3.1 and 6.3.2) are periodically reviewed to ensure that these continue to present a low risk of being used to evade tax.
- valid self-certifications are always obtained for New Accounts.
- Reporting Financial Institutions are followed up on when they report undocumented accounts.
- Financial Institutions, persons or intermediaries do not circumvent the due diligence and reporting procedures.

Where more than one authority is in charge of supervision, there should be a framework of co-ordination which ensures that there is a coherent overarching strategy, there is effective engagement among the authorities and there are no gaps in coverage.

Risk-based approach

The complexity and size of the financial industry as well as the resources of the supervisory authority(ies) render it difficult to conduct the same compliance activities for all Reporting Financial Institutions within the same period. It is therefore crucial to adopt a well-informed risk-based approach to prioritise resources to the areas of greatest risk in relation to the effective implementation of the AEOI Standard, both with respect to the Reporting Financial Institutions that might pose the greatest risk as well as focusing activities on the areas of greatest risk.

The risk assessment process should be documented and include an explanation of the factors considered and information sources used to take into account the determination of risks. Some of the possible factors include:

- the existing known risk profile of the financial sector
- the existence and strength of current supervision mechanisms
- current compliance with the AML/CFT regulations
- compliance with tax laws
- the timeliness, completeness and quality of reporting
- information on errors or suspected non-compliance received from partner jurisdictions (i.e. through notifications received under Section 4 of the CRS MCAA or equivalent).

The documented compliance strategy should describe the different steps to be followed, including the identification of the risks, their prioritisation, treatment and follow-up as well as the evaluation of the relevance of certain risks over time.

Desk-based audits and on-site audits

One critical component of the compliance strategy is to verify that Financial Institutions fully comply with the requirements of the Standard in practice. Verification activities can be conducted through both desk-based and on-site audits, with the objective of ensuring that Financial Institutions are (i) reporting as required and that (ii) the information reported is complete and accurate. For example, with respect to the Financial Account information collected, the audits should ensure that the key data points of the TIN and dates of birth are always obtained when required under the Standard. Furthermore, it should be ensured that authorities have the powers needed to conduct such verifications, including in relation to the full range of Financial Institutions under the Standard (i.e. both regulated and non-regulated Financial Institutions).

Some other aspects to be closely verified are as follows:

- procedures in place to verify that self-certifications are always obtained for New Accounts
- undocumented accounts: to understand the reasons for being reported as undocumented, ensure that the definition has been correctly applied, and ensure that the necessary, ongoing due diligence activity continues to be applied
- detection of circumvention and addressing it when identified

- verification of the correct application of the Non-Reporting Financial Institutions and Excluded Accounts categories. The verification should examine whether the business activities of Non-Reporting Financial Institutions meet the CRS criteria and whether they have correctly classified themselves. The verification process should also ensure that the list of Excluded Accounts is being correctly applied by Financial Institutions.

7.1.4. Applying sanctions as appropriate

Implementing jurisdictions are expected to have in place effective enforcement mechanisms to address non-compliance by Reporting Financial Institutions. While jurisdictions may initially adopt a cooperative ("soft landing") approach, there must also be legal and administrative mechanisms to allow the supervisory authority(ies) to sanction non-compliance with the CRS requirements when non-compliance is detected. This includes:

- identifying the authority(ies) in charge of applying the sanctions and ensuring they have the powers to apply them to the full range of Financial Institutions (i.e. both regulated and non-regulated Financial Institutions)
- communicating the possibility of sanctions as part of the education activities.
- developing the procedures to notify Reporting Financial Institutions when non-compliance is detected and impose the actual sanction
- recording, and in the case of financial penalties, accounting for and collecting the penalties

The procedures should ensure that the enforcement measures are applied in a timely manner including when different enforcement authorities are involved.

7.1.5. Collaborating with exchange partners on compliance and enforcement

One source of information that jurisdictions can use to detect potential non-compliance is information received from partner jurisdictions. When utilising the information received from an exchange partner, the receiving jurisdiction may detect errors or suspected non-compliance by a Reporting Financial Institution located in the jurisdiction sending the information. The receiving jurisdiction is expected to inform the sending jurisdiction of such errors or suspected non-compliance.

As part of its compliance strategy, jurisdictions are also expected to have procedures to follow up on any communication from exchange partners of errors or suspected non-compliance (e.g. through notifications received under Section 4 of the CRS MCAA or equivalent). Where such communications are received, jurisdictions are expected to process and address the issues raised by the exchange partners. This could include contacting the concerned Financial Institution to clarify the issues and obtain updated or corrected information where necessary, that should be resent to the partner jurisdiction. Responses are expected to be provided within 90 days of having received the notice, with updates provided within 90 days if the issue has not been resolved. Jurisdictions can allocate a responsible person or unit to follow-up on notifications, tracking all notifications received and ensuring that a response and subsequent updates are provided in a timely manner.

7.2. EXCHANGING INFORMATION EFFECTIVELY

The domestic legal framework introduces the obligation on Financial Institutions to report information to the competent authority in the jurisdiction. In order to comply with this obligation, the jurisdiction will need to put in place a mechanism to facilitate this domestic reporting. Once the jurisdiction receives this information from its Financial Institutions, it will then need to be able to exchange the information in a manner that not only meets the requirements of the Standard but is also efficient and secure.

Jurisdictions often prefer to meet these objectives by putting in place one comprehensive technical solution, supported by manual processes, to collect the domestic data from Financial Institutions and to prepare the data in line with the requirements before finally sending it to partners. The technical solution should include carrying out checks to ensure data quality, and preparing files in line with the required format for onward exchange to each partner jurisdiction. Such IT systems can also be developed to link with the CTS to transmit the files directly to exchange partners as well as to receive files from partners.

This section of the toolkit includes an overview of the key considerations in respect of developing an

IT solution (usually called an AEOI portal) to facilitate effective and efficient reporting by Financial Institutions and exchanges with partner jurisdictions.

It further outlines each of the key steps in the data handling and preparation process that jurisdictions should look to undertake in order to ensure information is exchanged effectively. This includes steps in relation to:

- receiving data from the Financial Institutions
- preparing data to be sent to the partner jurisdictions
- exchanging data with partner jurisdictions.

This section is intended to illustrate the main steps to exchange information in a simplified, "bite-sized" manner and it is not intended to act as the key reference point for these steps or for the development of an AEOI portal. Full details on these steps are available in the CRS XML schemas and CTS documentation referred to in this toolkit.

7.2.1. Developing an IT solution: the AEOI portal

Jurisdictions have typically sought to develop a comprehensive IT solution (AEOI portal) to fulfil all aspects of the domestic reporting and international exchange processes. Such IT solutions usually include:

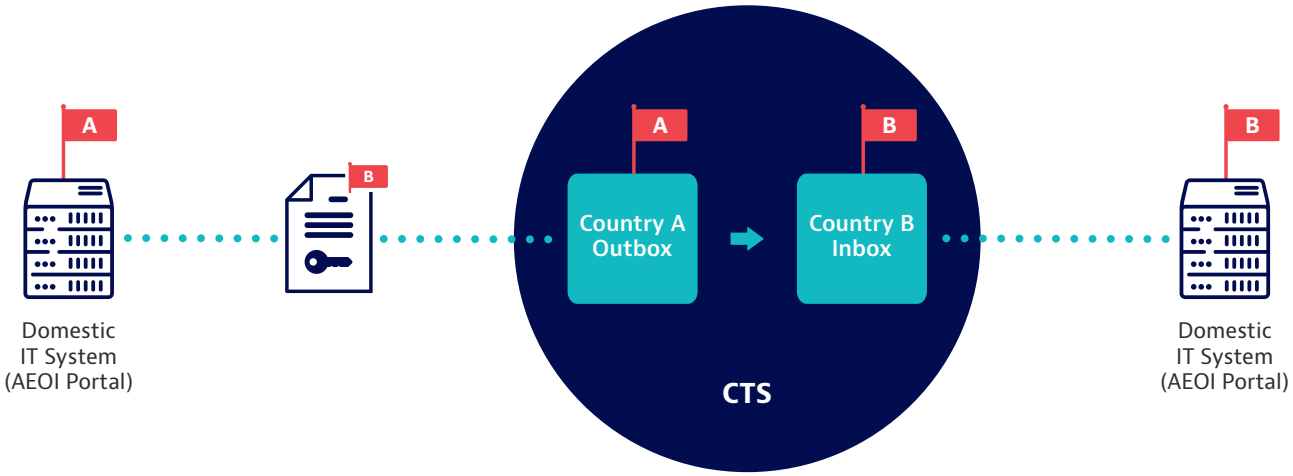
- a "customer interface" where Financial Institutions can submit their CRS data for onward exchange
- functionalities to carry out validation checks to ensure data quality
- functionalities to prepare the data packages for each jurisdiction's exchange partners
- functionalities to connect to the CTS to allow seamless transmission of the data from the AEOI portal to the jurisdiction's partners and reception of inbound CRS packages from its exchange partners
- functionalities to allow data analytics to be carried out as part of a jurisdiction's administrative compliance framework (see Box 16).

Figure 15 gives a visual representation of the AEOI portal and its connection to the CTS.

When developing an AEOI portal, the key decisions a jurisdiction will have to take are in respect of:

- building or buying an AEOI portal
- the functional requirements
- the technical requirements, including IT security considerations.

FIGURE 15. **How jurisdictions link to the CTS**



Note: Jurisdictions are able to link their domestic AEOI portals to the CTS using an SFTP or API function. In such cases, their AEOI portal will prepare a specific file for its partner jurisdiction, encrypt this file, before it is transmitted through the CTS to the exchange partner. If the receiving jurisdiction has also linked its systems to the AEOI portal, it will be able to receive the encrypted file directly. The system therefore permits end-to-end transmission without needing to directly access the CTS.

Deciding whether to build or buy an AEOI portal

The most significant strategic decision jurisdictions will need to make is whether to build a bespoke system (with internal capacities or by using outsourced IT development service provider), or to use an already developed ("off-the-shelf") system from an existing vendor. This decision may be made based on the jurisdictions' IT resources, features to be included in the AEOI system including any jurisdiction specific functionality, cost considerations, business requirements and security issues (including service level agreements (SLAs), non-disclosure agreements (NDAs), maintenance, and availability). Table 23 gives an overview of benefits and challenges for both approaches.

The "build" approach

Where a jurisdiction opts for the "build" approach, it may follow two different routes.

- The jurisdiction can develop the AEOI portal internally. In that case, it should make sure that it has adequate in-house IT development resources with relevant skills who can work on the project, as well as a solid understanding of the functionalities that the portal should have.
- The jurisdiction can also outsource in full or in part the development of the AEOI portal to external contractors where such in-house resources are not available. In such cases, it is critically important to:
  - have an adequate service contract for the IT system development activities (i.e. an SLA)
  - consider the ongoing activities that will be needed for system maintenance and upgrades
  - take into account some key security considerations when engaging contractors for development.

Box 14 illustrates some of the considerations that should be taken into account when designing the contracts.

The experiences for building an AEOI portal have differed between jurisdictions. For some, engagement with other tax authorities has been helpful in defining the technical specifications, allowing the development process to be completed in under six months. For others, it has taken as long as one to two years to develop their own IT solution.

Table 23. **Buy versus build**

	Buy (off-the-shelf)	Build (custom / bespoke)
Benefits	• Quicker implementation • Easy maintenance • No in-house IT development resources needed	• Better fit to specific requirements of the jurisdiction • Leverage on existing infrastructure and expenses for staff • Confidentiality requirements can be ensured by design • Quick feature development
Challenges	• Need to create request for proposals, SLAs, NDAs • Complex addition of new/customised functional requirements • Recurring cost for both implementation and maintenance • Possible issues with data portability and additional confidentiality considerations	• Complex development as good understanding of the requirements is needed • Need for in-house IT development resources • Need for regular maintenance • In case outsourced development or maintenance, need to create request for proposals, SLAs, NDAs

Box 14. **Key contractual considerations for outsourced development of the AEOI portal**

When engaging an external provider to complete, or to support, the development of the AEOI portal, jurisdictions should take into account the following key contractual considerations to ensure a more successful engagement.

- **Selecting the type of contract:**
  - Fixed price contracts – these specify the scope of the project (i.e. the requirements and costs of the system). A flat rate will apply regardless of the staff time spent or resources used.
  - Time and materials contracts – these do not fix the price nor the scope of the project, but set out the conditions in respect of the staff resource and the material that will be needed to carry out the work. The price is based on the agreed-upon rate applied to the actual resources used and time spent.
- **Selection of the methodology for development of the AEOI portal:**
  - Agile methodology – the requirements are defined in an incremental and iterative process. Each iteration (sprint) has its own testing phase (i.e. the functionalities are available for testing in each sprint and can be used afterwards). User acceptance is performed at the end of every sprint. The duration of the development is generally uncertain.
  - Traditional "waterfall" methodology – the requirements are defined at the beginning of the project. All functionalities are available for testing at the end. User acceptance is performed at the end of the development. The duration of the development is usually predefined.
- **Competence and experience of the development team:** the profiles (project manager, architect, developers, testers, etc.) and their qualifications required for the development of the AEOI portal should be defined in the contract.
- **Rights of use:** the contract should set out who has the exclusive right to use the software being developed, as well as who has the right to modify it (such as by the jurisdiction's developers or any other contractor engaged by the jurisdiction in case of a change of suppliers). Where proprietary or open source libraries are used as part of the code, the rights to use this code should be clearly defined.
- **Use of open source components:** the contract should forbid the use of open source components with "copyleft" license as their use is very restrictive, and should require that the development is done in a manner to ensure separation of the libraries from the code base.
- **Source code:** the contract should require the transfer of source code for the developed solution so that further changes can be made internally or by another supplier.
- **Testing and validation (acceptance criteria):** the contract should define what type of testing and validation will be done, and by whom. Some types of tests can include unit testing, accessibility testing, and integration testing. Additionally, end user testing is also an important feature.
- **Documentation:** the requirements for documentation to be provided by the supplier and level of detail should be defined in the contract. This typically includes technical, user and project documentation.
  - Technical documentation can be included as inline comments in the source code and as separate documentation.
  - Project documentation is especially important in time and material contracts, as it can provide supporting evidence for the "level of effort" used in the project.
  - Technical and user documentation should be updated by the supplier as often as the source code, while project documentation should be continually accessible for the duration of the project. At the end of the project, a complete set of technical, user and project documentation should be delivered together with the source code and other installation components.
- **Penalties for delays:** these should be defined in the contract. A definition on what is an acceptable delay can also be set out for situations where delays may be justifiable.

Source: Global Forum Secretariat / OECD (2021), *Capacity-Building Tool: Guidance on AEOI Portal Design and Development*, available to competent authorities on request.

The "buy" approach

If a jurisdiction chooses to take the "buy" approach, it will have to balance various criteria including: cost, reputability, scope of functionalities, scalability, reporting options and any domestic requirements on procurement.

In all cases, it is good practice to carry out market research to identify possible vendors and to conduct due diligence of the preferred vendor before engaging its services. It can also be helpful to reach out to partner jurisdictions to learn from their experiences with their vendors.

After the selection of the vendor, the contracting should be done with due care to cover not only the general aspects but also the specificities of the AEOI portal. There are some key security considerations to make when purchasing off-the-shelf IT solutions. Box 15 illustrates some of the considerations that should be taken into account when taking this approach and developing contracts for this purpose.

Box 15. **Some key considerations in service contracts for using off-the-shelf AEOI portal**

When engaging an external service provider to provide a complete off-the-shelf IT solution, jurisdictions may want to take into account the following key contractual considerations in order to ensure a more successful engagement.

- **Hosting of the AEOI portal:**
  - Cloud based: the AEOI portal will be provided as an online service where the Financial Institutions (for submission of CRS data) and the competent authority (for management and preparation for exchange) access it via a web browser. The vendor will also have access via a web browser for setup and maintenance. The data is stored in a cloud from a reputable cloud supplier, or in the jurisdiction's government cloud.
  - On-premise: the AEOI portal is installed on the IT infrastructure of the tax administration, and it can be accessed by the Financial Institutions (to submit CRS data) and the competent authority (for management and preparation for exchange) via a web browser. The vendor or tax administration can access it via an administration console or a web browser (to carry out maintenance). The data is stored in the tax administration data centre.
- **Technical specification:** even though the AEOI portal is provided as an off-the-shelf solution, its features and functionalities should be defined and documented in the contract or its associated documentation. This is specifically important as the portal would need to be customised for the specificities of the tax administration.
- **Testing:** penetration testing or source code testing should either be disclosed by the vendor or be allowed to be done by the tax administration's own IT employees or contracted specialised service provider.
- **Warranties and service levels:** these aspects depend on the criticality of the system for the operations of the jurisdiction. Hours of operations, service quality, service availability and downtime are some of the items that should be defined in the contract. Penalties for not meeting the defined service levels should also be defined. The availability of the AEOI portal is critical during the peak period of collection of information from the Financial Institutions and the period when the exchanges take place.
- **Maintenance:** the contract should set out the expectations and requirements in respect of updates, upgrades and patches for the various functionalities. It should also specify the timeframe and the cost of any maintenance activities.
- **Ownership and protection of data:** measures necessary to ensure the confidentiality of the data should be clearly defined in the contract in respect of data submitted domestically by Financial Institutions, and any inbound data from exchange partners the system will receive. Specific clauses should exist on the portability of data in case the jurisdiction decides to change the AEOI portal and its supplier in the future. Data in production environment should be kept encrypted with keys from the tax administration and should not be accessible by the vendor, unless adequate security measures are defined and implemented, and the access is regularly audited.
- **Business continuity:** the contract should set out what provisions should be in place in case the vendor goes out of business or ceases operations. Provisions may allow for the transfer of the source code of the system to the tax administration, or timely notification requirements and data portability options.

Source: Global Forum Secretariat / OECD (2021), *Capacity-Building Tool: Guidance on AEOI Portal Design and Development*, available to competent authorities on request.

Determining the functional requirements

Regardless of the selected approach ("build" or "buy"), the AEOI portal should provide similar business functionalities and have comparable security features. It can allow for some integration with internal systems or interoperability with systems for other exchanges.

In terms of business functionalities, jurisdictions should ensure that all reporting and exchange requirements can be adhered to by the Financial Institutions which have an obligation to report domestically and by the jurisdiction which must meet the requirements for exchange, including the sending of any CRS Status Messages. These requirements are set out in the CRS XML Schema User Guide[72] and the CRS Status Message XML Schema User Guide.[73]

The system should also include functionalities which allow for effective interaction with the Financial Institutions and quality controls of the data they submit, as well as for the generation of any statistics required or helpful for ensuring compliance (see Box 16). Jurisdictions will also wish to consider any functionalities needed to

72. The CRS XML Schema Version 2.0 and the CRS User Guide Version 3.0 for Tax Administrations are available at www.oecd.org/tax/automatic-exchange/common-reporting-standard/schema-and-user-guide.

73. The CRS Status Message XML Schema Version 2.0 and the CRS Status Message XML Schema User Guide for Tax Administrations Version 2.0 are available at www.oecd.org/tax/automatic-exchange/publications/common-reporting-standard-status-message-xml-schema-user-guide-for-tax-administrations.htm.

Box 16. **Considerations in respect of a jurisdiction's administrative compliance framework**

Jurisdictions are required to have in place an administrative compliance framework to ensure that its Financial Institutions are complying with their due diligence and reporting obligations in practice (see Subsection 7.1 of the toolkit). While development of a jurisdiction's overall compliance framework might commence at a later stage in its implementation of the Standard, jurisdictions should still reflect on how they will use their AEOI portal, and the information received from Financial Institutions, to ensure compliance.

Some key considerations for jurisdictions when determining the specifications of their AEOI portal should be:

- ensuring the registration of Reporting Financial Institutions
- ensuring that the information reported by Financial Institutions can be readily accessed for risk assessment and risk working purposes to verify compliance. In practice, this may include:
  - identifying accounts which have been reported out of line with expectations (such as what is already known by tax administration in respect of the account or the Financial Institution)
  - extracting accounts to allow sampling checks to be undertaken as part of verification activities
  - identifying all Financial Institutions which have reported, to allow this information to be cross checked with other available information for the purposes of identifying which Financial Institutions incorrectly did not report
  - identifying Financial Institutions that have reported late
  - identifying Financial Institutions which submitted CRS files that were rejected
  - ensuring that correction files have been submitted by a Financial Institution following verification activities and the identification of any errors
- ensuring that Financial Institutions which report accounts as "undocumented accounts" can be easily identified. This will allow jurisdictions to follow up undocumented accounts to establish the reasons why such information is being reported.
- collecting key data points for developing an effective compliance strategy, including:
  - the number of Financial Institutions that have reported
  - the number of Financial Accounts that been reported (overall and by Financial Institution)
  - the number of Financial Accounts reported without TINs (overall and by Financial Institution)
  - the number of Financial Accounts reported without dates of birth (overall and by Financial Institution).

ensure successful interoperability with other systems used by the tax administration (see Box 17). A key part of the AEOI portal will be the user interface where Financial Institutions can submit their CRS data. Close cooperation with Financial Institutions by allowing them the opportunity to provide input on the design process of the user interface, has been considered by some jurisdictions to be a critical success factor in ensuring that it can be used easily and effectively by users.

Table 24 presents some high-level business functionalities for the development of an AEOI portal to consider.

Table 24. **Some high-level business functionalities for the development of an AEOI portal**

Functionalities	Description
Functionalities relating to receiving CRS information from Financial Institutions	• Registration of Financial Institutions: identification and verification of Financial Institutions and their authorised users. • Safety check of data to be submitted by mandatory antivirus scanning prior to submission. • Secure submission of CRS data from the Financial Institutions (e.g. server-to-server link-up (Simple File Transfer Protocol – SFTP), browser-based manner (Hyper Text Transfer Protocol Secure – HTTPS)) and generating adequate confirmation messages (i.e. messages sent to Financial Institutions to confirm acceptance or rejection of file; in cases of rejection, these could specify the reason for rejection). • Function to communicate with individual Financial Institutions in respect of the information they submit, as part of compliance activities, or where troubleshooting issues are experienced by Financial Institutions. • Quality control of submitted data which should include at a minimum, validation checks to ensure information meets the CRS XML schema requirements (see Subsections 7.2.2 and 7.2.3 of the toolkit). • Ability to carry out sense checks (see Subsection 7.2.3 of the toolkit) on data submitted by Financial Institutions for any errors.

Functionalities relating to sending CRS data to AEOI partner jurisdictions and receiving CRS data from them	• Function to prepare, validate and encrypt packages for exchange partners.
	• Management of public and private keys and integrating the encrypting and decrypting process.
	• Ability to analyse the data received and carry out risk assessments for purposes of ensuring compliance of Financial Institutions with the due diligence and reporting requirements (see Box 16).
	• Function to manage corrections in CRS files: matching of CRS corrections to original CRS files. Where a CRS file is amended, either by the tax administration or resubmitted by the Financial Institution, the system should be able to produce a complete record of the transaction.
	• Viewing all sent and received files to manage queries.
	• If a jurisdiction intends to transmit the information through the CTS via server-to-server link-up (SFTP) function, the system will also need to incorporate the relevant specifications to link to the CTS (See Subsection 7.2.4). Functional requirements will be needed in respect of:
	  - connectivity to the CTS
	  - receiving CRS Status Messages from exchange partners once they have received your jurisdiction's data
	  - generating and sending CRS Status Messages to partner jurisdictions following the receipt of their data
	  - receipt of data through the CTS, decryption, validation, preparation and sending of a CRS Status Message.

Considerations for security requirements

Security requirements for the development of the AEOI portal should be based on international best practices and concepts such as "security by design" and "privacy by design", and should reflect the applicable requirements on confidentiality and data safeguards from the related ToR (see Subsection 2.2.3 of the toolkit). Furthermore, similar security requirements in line with these ToR should be reflected in the activities of the jurisdiction after the portal is put into production.

High-level security considerations include:

- Adhering to security by design and privacy by design principles allowing for the data safeguards to be integrated into the design of the AEOI portal.
- Adhering to good application design practices such as having separate production, testing and development environments, using dummy data for testing, performing code reviews and producing detailed technical and user documentation.
- Ensuring protection of confidentiality of data by implementing mandatory encryption of data in transit to prevent eavesdropping and for the data at rest in the backups to protect from data leakage. If feasible, it is as highly recommended to encrypt data in the databases themselves that is actively used, but this decision should be made after considering the need to access and use the data in daily activities. Additionally there should be adequate functionalities for management and storage of encryption keys.
- Adequate background checks and vetting of development, testing and maintenance teams in line with local legislation and their involvement in the development process.

Box 17. **Interoperability of AEOI portal (with other forms of exchange and internal systems)**

EOI for tax purposes is a developing area. Similar to CRS-AEOI, some other forms of exchanges require third parties to provide the tax administration with information on a periodic basis for exchange. As such, when developing an AEOI portal, jurisdictions may want to consider the potential for (future) portal adaptations to facilitate reporting for instance in respect of:

- Country-by-Country Reporting (CbC)[1]
- Mandatory Disclosure Rules on CRS Avoidance Arrangements and Opaque Offshore Structures (MDR)[2]
- Exchanges on Substantial Activities in No or Only Nominal Tax Jurisdictions (NTJ)[3]
- Automatic Exchanges of Information Derived through Digital Platforms (DPI)[4]

It is also important to note that the CRS XML Schema develops over time and any AEOI portal should be able to incorporate such developments and to perform the additional validations set out in the CRS Status Message User Guide.

Reciprocal jurisdictions may also look to ensure that the IT solution developed for these exchanges is operable alongside any existing taxpayer systems used to allow for effective matching and for compliance activities. Application Programming Interfaces (APIs) allow for increased interoperability between the AEOI portal and domestic taxpayer systems. An API could allow information from an individual's tax record to be identified and used in the matching process for instance. Interoperability with any EOIR software might also be considered for the management of follow-up requests.

Note:

1. CbC Reporting XML Schema Version 2.0 and its User Guide for Tax Administrations Version 2.0 are available at www.oecd.org/tax/country-by-country-reporting-xml-schema-user-guide-for-tax-administrations.htm.

2. MDR XML Schema Version 1.0 and its User Guide are available at www.oecd.org/ctp/exchange-of-tax-information/international-exchange-framework-for-mandatory-disclosure-rules-on-crs-avoidance-arrangements-and-opaque-offshore-structures.htm.

3. NTJ XML Schema and its Guidance for the Spontaneous Exchange of Information are available at www.oecd.org/tax/beps/substantial-activities-in-no-or-only-nominal-tax-jurisdictions-guidance-for-the-spontaneous-exchange-of-information.htm.

4. DPI XML Schema and User Guide are expected to be released early 2022.

- Designing granular access control both for end-users and administrators of the system (authentication and authorisation) so that the access provision can be done in line with "need to know" and "least privilege" principles. The granularity should also be reflected in the permissions on working with the data, i.e. create, read only, modify, delete or similar.
- Detailed logging of all access and changes to data in the AEOI portal.
- Possibility to define customised monitoring alerts on the logs that flag unusual transactions or access to reflect the internal policies and sensitivity of the data.
- Penetration testing of internal and external interfaces.
- Regular patching and robust change management processes.
- Adequate data structure and processes for enabling data portability.
- Integrated backup processes for both system and data in the databases.

The Global Forum has developed a more detailed description of the functional and security considerations for the AEOI portal design.[74] It is available on request to competent authorities by contacting gfconfidentiality@oecd.org.

7.2.2. Obtaining information from Financial Institutions

A central feature of the AEOI portal is the collection of data on Reportable Accounts provided by Reporting Financial Institutions. The main functions to be performed by the portal are:

- registration of Financial Institutions (and their appointed representatives) into the system
- receiving the data files submitted by Financial Institutions (including receiving nil reports if required)
- validating the data provided by Financial Institutions.

Registration of Financial Institutions

Upon the full implementation and operationalisation of an AEOI portal, Reporting Financial Institutions will be required to register before submitting CRS data.

As part of this registration, AEOI portals typically require institutional information in respect of each Financial Institution (such as the name, address, phone number, and any business registration or tax identification number) as well as information in respect of an appointed representative (or designated user). This information will be key to allowing the Financial Institution to submit CRS data and the jurisdiction to follow up with their Financial Institutions for compliance purposes, following the submission of CRS files.

Depending on how the jurisdiction wants to grant access to individuals within Financial Institutions for data uploads, the appointed representative for each Financial Institution could be the sole person with access to the portal for data submission on the Financial Institution's behalf, or could be responsible for allocating further user profiles within their institution. The appointed representative can also act as the point of contact between the Financial Institution and the tax administration on all matters related to the submission of information.

Receiving data files from Financial Institutions

The domestic legislative frameworks to implement the Standard will set out a deadline by which Reporting Financial Institutions are required to submit the CRS data (the filing deadline). This deadline must be sufficiently early to ensure that the jurisdiction is in a position to exchange within nine months following the end of the calendar year to which the information relates. Therefore, for a given reportable year (Y), jurisdictions have from 1 January Y+1 until 30 September Y+1 to:

- collect the data from Financial Institutions
- perform additional checks and procedures to prepare the data for exchange
- share the data with their exchange partners.

Full details on selecting a reporting deadline for Financial Institutions are set out under Subsection 6.3.2 of the toolkit.

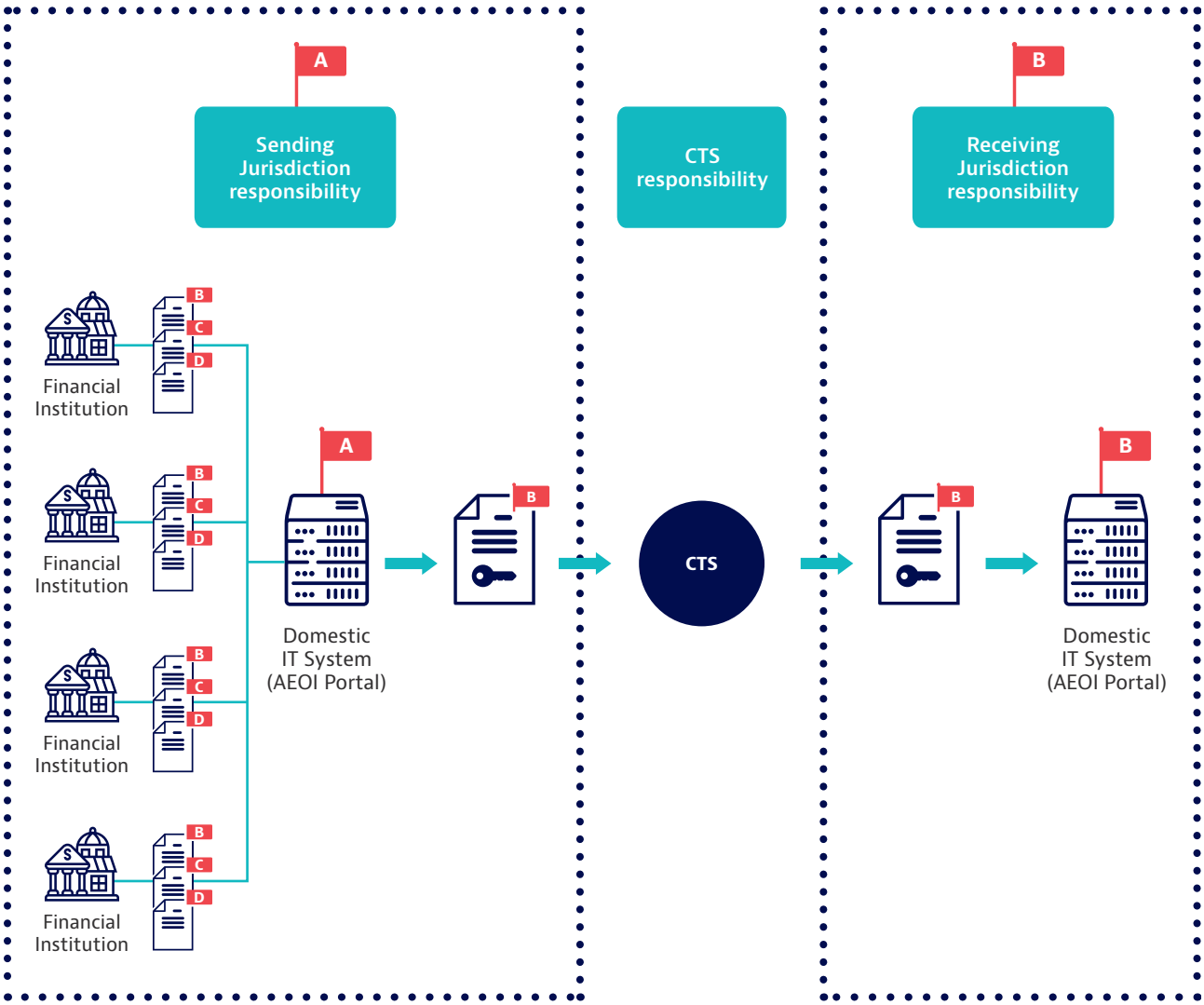
It is for the jurisdiction to determine the format in which its Financial Institutions provide CRS data. They have often required Financial Institutions (or required those Financial Institutions submitting information concerning a large number of accounts) to submit the data fully conforming to the same CRS XML Schema format that the jurisdiction must use when sending the data to its partner jurisdictions.

74. Global Forum Secretariat / OECD (2021), *Capacity-Building Tool: Guidance on AEOI Portal Design and Development*.

When developing an AEOI portal, there are generally two ways jurisdictions will permit the upload of XML Schema files and these will depend on the system functionality to convert the files into jurisdiction-specific packages.

1. Financial Institutions can be required to submit data in **jurisdiction-specific files** (i.e. a Reporting Financial Institution will submit one file for each jurisdiction of residence of the Reportable Persons). This will make it easier for the sending jurisdiction to consolidate all files received by Reporting Financial Institutions relating to each jurisdiction of residence when preparing packages for its exchange partners. This is a necessary feature when this consolidation must be done manually because the AEOI portal does not have a functionality to extract a particular jurisdiction's accounts from each file submitted for consolidation. In any case, the competent authority must still check each file prepared for jurisdictions before sending to ensure that it only contains records that are destined for the relevant jurisdiction. This approach usually limits errors in the preparation of the files to be exchanged with exchange partners as it reduces the number of interventions in respect of the data received. Figure 16 illustrates this approach.

FIGURE 16. **Jurisdiction-specific file submission**



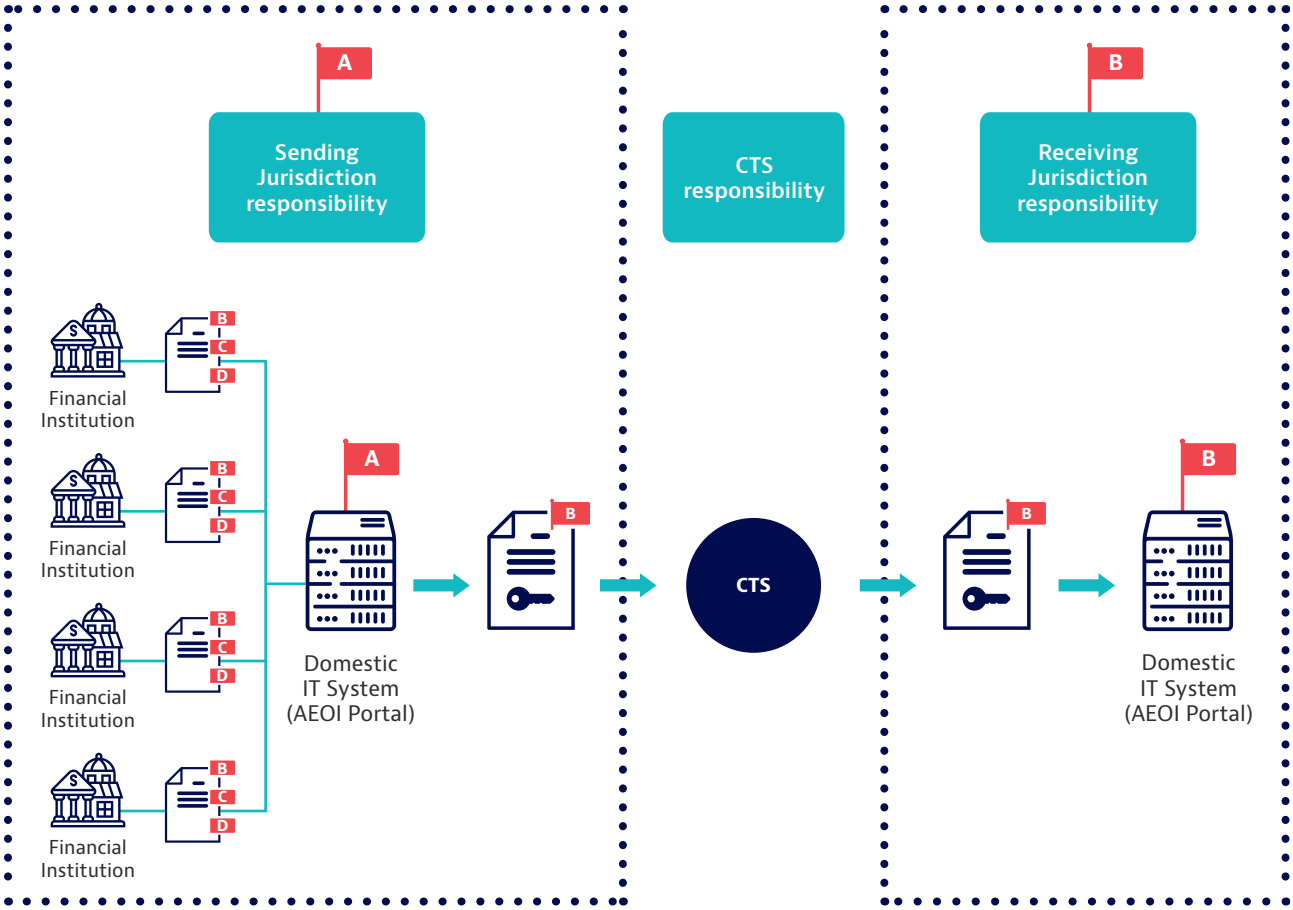
Note: In this example, Jurisdiction A has set up their system to require its Financial Institutions to submit files which only include Reportable Accounts in respect of one Reportable Jurisdiction. Therefore the Reporting Financial Institution will submit one or more files per Reportable Jurisdiction for which it has Reportable Accounts. Jurisdiction A's system will merge files in submitted by Financial Institutions in respect of Jurisdiction B and prepare a Jurisidiction B file for exchange. The Note to Figure 15 details the remaining steps in transmission.

2. Financial Institutions may be allowed to submit data files with **all jurisdictions'** Reportable Accounts **consolidated into the same file** (i.e. a Reporting Financial Institution submits a file containing all the Reportable Accounts it maintains irrespective of the jurisdiction of residence of the Reportable Persons). When a jurisdiction is ready to prepare a package for sending to a partner jurisdiction, the AEOI portal will extract all accounts reportable to that particular jurisdiction from the pooled information submitted by its Financial Institutions. This approach can reduce compliance costs for Financial Institutions and manual resource needed by the tax administration, however it requires more advanced functionality within the AEOI portal. Figure 17 illustrates this approach.

Some jurisdictions also permit the filing of CRS data in additional formats, including through easy-to-use online forms or with excel spreadsheets. In such cases, as it would be extremely burdensome on the jurisdiction to manually format this data for exchange purposes, these jurisdictions have developed in-built conversion tools and require that individual fields be populated in the exact same manner as required by the CRS XML Schema, which must always be used when exchanging the information internationally (e.g. every date of birth field must be populated YYYY-MM-DD). This functionality may be useful for Reporting Financial Institutions which have only a low number of accounts to report as it can help limit their compliance costs and improve compliance.

Jurisdictions, which choose to allow the submission of CRS information from Financial Institutions via other formats (spreadsheets or via a web form) usually integrate these formats into the AEOI portal. They will have to consider how the portal's functionalities will

FIGURE 17. **Consolidated jurisdiction file submission**



Note: In this example, Jurisdiction A has set up their system to allow all its Financial Institutions to submit files including all Reportable Accounts (i.e. those to be exchange to all Reportable Jurisdictions). Jurisdiction A's system will extract all Jurisdiction B Reportable Accounts from all submitted files and include these into a Jurisdiction B file which it will prepare for exchange. The Note to Figure 15 details the remaining steps in transmission.

allow this information to be extracted and added to the jurisdiction-specific packages for exchange.

A key aspect that should not be overlooked in the development of an AEOI portal is ensuring that even outside of the typical reporting period (between 1 January and the domestic filing deadline), Financial Institutions will still need to be able to submit CRS files. This includes Financial Institutions that are filing late, but also cases where the Financial Institution is required to submit correction files. Correction files might be submitted when the Financial Institution identifies issues on its own accord or when corrections are required following compliance activity. Such correction files are different from files which Financial Institutions are required to re-submit following failures in validation. Further information on ensuring correction files are in line with the requirements is available in the CRS XML Schema User Guide.

Data validation

When a Financial Institution submits the data through the AEOI portal, the system should perform a key quality control function by validating the information presented to ensure it meets the CRS XML Schema requirements and the requirements for additional data validation set out in the CRS Status Message User Guide. This includes ensuring that the obligatory schema elements are present for all Financial Accounts reported and that they are populated in the correct format (i.e. validation of the format of the data to ensure that it has been entered correctly, with the mandatory information included) as well as the relevant additional file and record validations. To that end, the jurisdiction can apply the guidance provided in the CRS XML Schema User Guide and the CRS Status Message XML Schema User Guide for using these Schemas for the domestic submission of data by Financial Institutions.

If the jurisdiction also implements a requirement for encryption on the files submitted and communication between Financial Institution and tax administrations through the AEOI portal, the validation tool may also carry out a check on the digital signature or electronic certificate of the submission (see Box 18).

In case the data submission cannot be validated due to significant errors related to such issues, the AEOI portal should reject the file to be submitted by the Financial Institution (prevent submission). Ideally the Financial Institution would be informed of the error(s) in the file leading to rejection. This can be done via an automated message on file upload.[75] The Financial Institution can then address the identified errors and provide a corrected file submission. Figure 18 illustrates the data validation on file submitted by Financial Institutions.

While the AEOI portal can be designed to include the sending and receipt of messages between the tax administration and the Financial Institutions, tax administrations may also wish to put in place other means of communication such as a dedicated email or hotline, that Financial Institutions can contact to raise any issues in relation to the data submission, or for any other compliance purposes.

75. Some jurisdictions refer to these messages as status messages, however the term is not used here to prevent confusion with "CRS Status Messages" which are sent between jurisdictions.

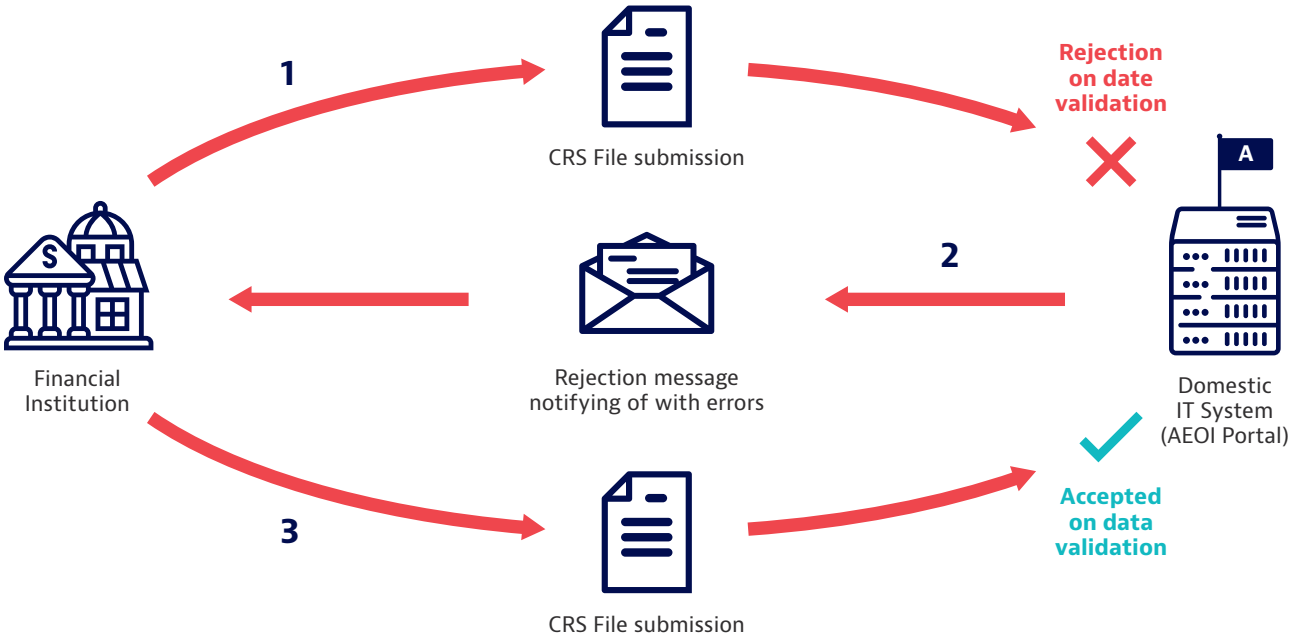
Box 18. **Encryption for data collection from Financial Institutions**

In all aspects of the development of an AEOI portal, the jurisdiction should consider measures to ensure the confidentiality and safeguarding of the data, including data received domestically for onward exchange.

Jurisdictions must encrypt the packages to be exchanged to partner jurisdictions in line with agreed encryption standards for transmission. However, jurisdictions should also consider introducing similar encryption requirements in respect of the CRS files submitted by its Financial Institutions through the AEOI portal.

The Financial Institution to competent authority encryption must be separate and independent from the encryption that the jurisdiction must subsequently carry out for transmission to exchange partners. Where applied, the portal would have to decrypt the files received from Financial Institutions, consolidate the jurisdiction-specific information into jurisdiction packages, before encrypting each of these packages with a digital signature for transmission to exchange partners. Some jurisdictions have also included the verification of the digital signature or electronic certificate of the submission by Financial Institutions at the data validation stage.

FIGURE 18. **Data validation on Financial Institution file submission**



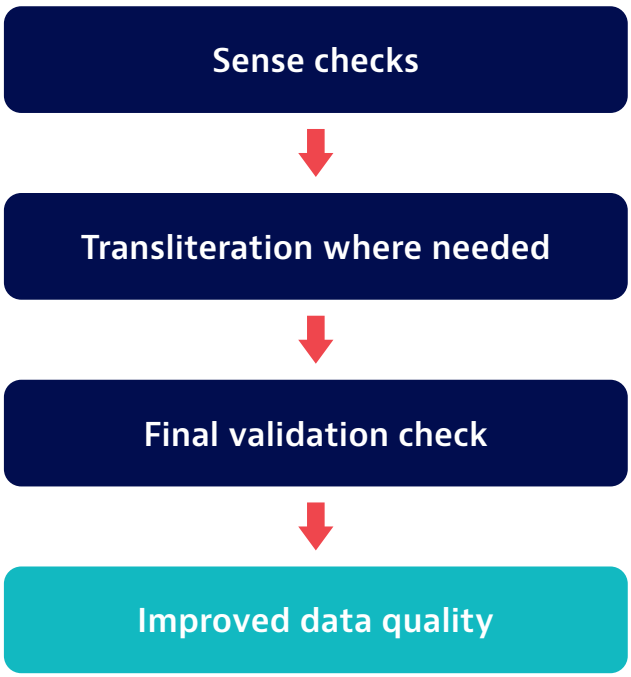
Note: In this example, the Financial Institution has tried to submit a file to Jurisdiction A's AEOI portal but it was rejected on submission because it did not meet the CRS XML Schema requirements and therefore failed validation. The AEOI portal then sends a message notifying the Financial Institution of rejection and stating why it failed the Schema validation. Once the Financial Institution has addressed the issue, it sends an updated file which passes the CRS Schema validation and is accepted by the AEOI portal.

7.2.3. Preparing data for the partners

Once the data has been submitted by the jurisdiction's Financial Institutions and these data files have been validated by the AEOI portal, the first step in preparing data to send to partners is to package files for each partner jurisdiction that only include accounts reportable to that jurisdiction. As mentioned under Subsection 7.2.2 of the toolkit, tax administrations will have to determine whether to enable their Financial Institutions to upload jurisdiction-specific files or consolidated files. This approach will be inherently linked to the functionality of the portal to extract the relevant reportable accounts from each Financial Institution file and to consolidate all accounts reported into jurisdiction-specific packages. As a general rule, one single package should be prepared for each receiving jurisdiction for each exchange cycle.

Once jurisdiction-specific packages are prepared, the sending jurisdiction should perform a series of checks to ensure data quality. This will limit the likelihood of files being rejected by exchange partners and of receiving notifications of any errors identified. Figure 19 illustrates these checks.

FIGURE 19. **Data quality checks**



Sense checks

Sense checks can help identify any anomalies in the data that a schema validation check would not detect. Reviewing key fields will help identify whether the Financial Institution has not provided a complete name or a full address (or populated fields with incorrect data intended to pass XML Schema validation), or provided data which is obviously erroneous (such as a test account or an account with an unexpectedly inflated account balance (e.g. TIN inserted in balance field)). Depending on the AEOI portal developed, and the number of Financial Institution submissions, the sending jurisdiction may prefer to carry out sense checks on the files submitted by Financial Institutions rather than on the packaged files.

Transliteration

In the case that both jurisdictions involved in the exchange do not use the Latin alphabet, jurisdictions may agree how they will undertake such transliteration. Jurisdictions should consider the alphabet used by the recipient jurisdiction and, if requested, it should transliterate from its domestic alphabet or literation to a Latin alphabet aligned with international standards for transliteration (for example as specified in ISO 8 859). Transliteration is an important step to ensure the data will not get distorted and can be processed by the recipient jurisdiction. Jurisdictions can also send the central aspects of the data – such as full name or address – in both the domestic alphabet and separately in Latin alphabet within each account record.

Final validation check

Once jurisdiction-specific packages have been created, incorporating all accounts reportable to that jurisdiction, it is good practice to once again validate the data against the CRS XML schema requirements and to perform the additional validations set out in the CRS Status Message User Guide before exchanging.

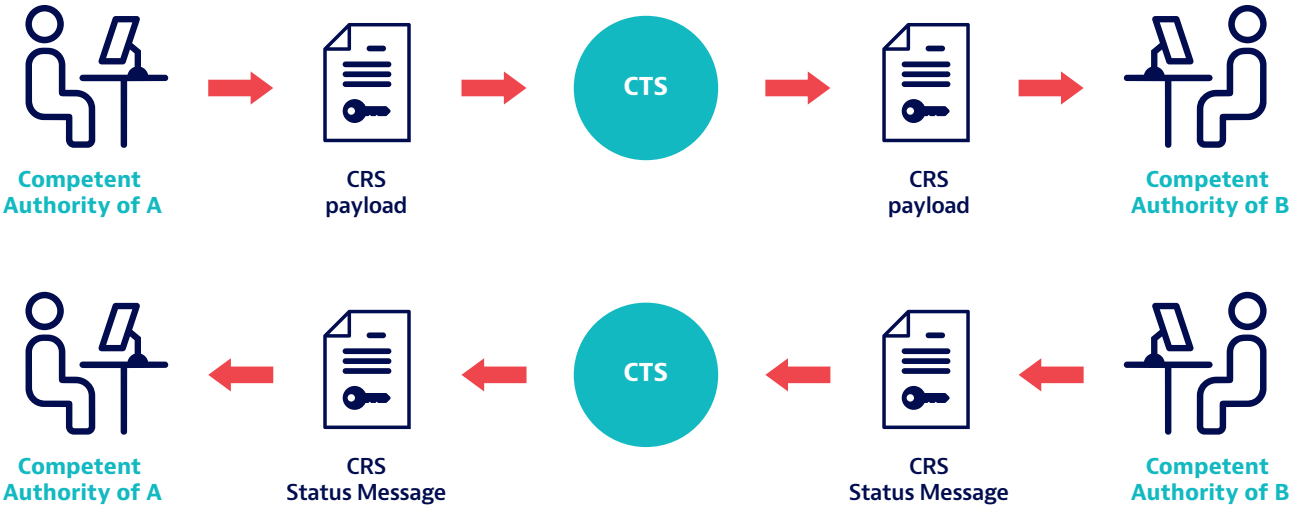
7.2.4. Exchanging the CRS data with partner jurisdictions

With jurisdiction-specific packages ready, the final steps to complete the exchanges of CRS data are to encrypt and transmit the packages. Similar steps in reverse will also be needed when packages are received from exchange partners before CRS Status Messages are sent.

Encryption

Depending on the AEOI portal and the size of the data to be exchanged (the maximum size of a payload file for CTS transmission is set at 250MB, but may be lower at the request of each receiving jurisdiction), the CRS data for a specific Reportable Jurisdiction may be packaged into one or multiple CRS XML files: these files, which include financial account information, are often referred to as "payload files". Prior to encryption of the payload file, the CRS XML file must be compressed. Each of the aforementioned steps must be carried out on every payload file that is to be sent to an exchange partner.

FIGURE 20. **Encryption and transmission of payload files and CRS Status Messages**



Note: In this figure, Jurisdiction A sends an encrypted file containing CRS information (a payload file) through the CTS which is received by Jurisdiction B. Jurisdiction B is expected to send an encrypted CRS Status Message back to Jurisdiction A which also can be sent through the CTS. The Status Message will indicate whether the file has been accepted or rejected and if there are any file or record errors.

Once a jurisdiction has received a payload file, it must confirm receipt and highlight any errors by sending a CRS Status Message to its partner. Each Status Message file should also be validated to ensure that it meets the CRS Status Message XML Schema requirements and it must also be encrypted before sending (see Box 19).

These steps are illustrated in Figure 20.

Jurisdictions which carry out transmissions through the CTS will follow its prescribed encryption requirements. This includes strict requirements outlined in the File Preparation and Encryption User Guide (made available to competent authorities with a User Agreement in place (CTS Users).

Jurisdictions should consider the most effective way to apply these encryption and decryption processes in the early stages of the development of the AEOI portal. While manual processes could be implemented to encrypt each file individually, the jurisdiction should consider the practical challenges of doing this in light of the number of files it anticipates sending and receiving.

Manual encryption (and decryption) processes would be particularly burdensome to implement for jurisdictions intending to exchange on a reciprocal basis or where there is likely to be a large number of Reportable Accounts resulting in multiple payload files for each exchange partner. Therefore jurisdictions should consider the benefits of developing a tool (or incorporating this functionality in their AEOI portal) to carry out the process of encryption and decryption on an automatic basis.

Transmission and the Common Transmission System

As set out in the CRS MCAA, jurisdictions exchanging information under the CRS need to agree and use the appropriate minimum standards with each exchange partner to ensure the confidentiality and integrity of the data throughout the transmission. While this requirement does not preclude other methods of transmission, the CTS has been used by all CRS exchange jurisdictions to transmit CRS data to exchange partners. This toolkit will therefore only focus on this method of transmission.

Box 19. **What is encryption?**

Encryption is designed to protect both the confidentiality and the integrity of the data. It transforms the data to render it unintelligible to anyone who does not possess the decryption key.

Public key cryptography is a standard method of encryption which uses both a public and a private key. The sending jurisdiction encrypts the data file with a public key, and only the receiving jurisdiction holds the secure private key that allows the data to be decrypted. There are standards for the length of encryption keys that are recognised as providing the appropriate level of security for data of this sensitivity, both now and for the foreseeable future, such as advanced encryption standard (AES) 256.

What is the difference between encrypting and signing?

- Encryption: making sure no else can read the file.
  - *Encryption is the process of encoding files (or other information) in such a way that only authorised parties can read it but so that any eavesdroppers or hackers cannot.*
- Signing: verifying the authenticity.
  - *Signing can be used to verify if the person who sent you the file is really the person who they claim to be (i.e. authentication of the sender) and if the file has been altered by another person.*

How does this work with the public/private keys?

When exchanging with an exchange partner:

- For encrypting, the sending jurisdiction will use the public key of their exchange partner to encrypt the message. The exchange partner will use their private key to decrypt the message.
- For signing, the sending jurisdiction will use their private key to provide a signature to the message. The receiving jurisdiction will use the sending jurisdiction's public key to verify the identity of the sender.

Since only the private key can decrypt the file, it must not be shared. Despite its name, the public keys for CTS encryption and transmission must not be made publicly available. They are accessible only to exchange partners through the CTS.

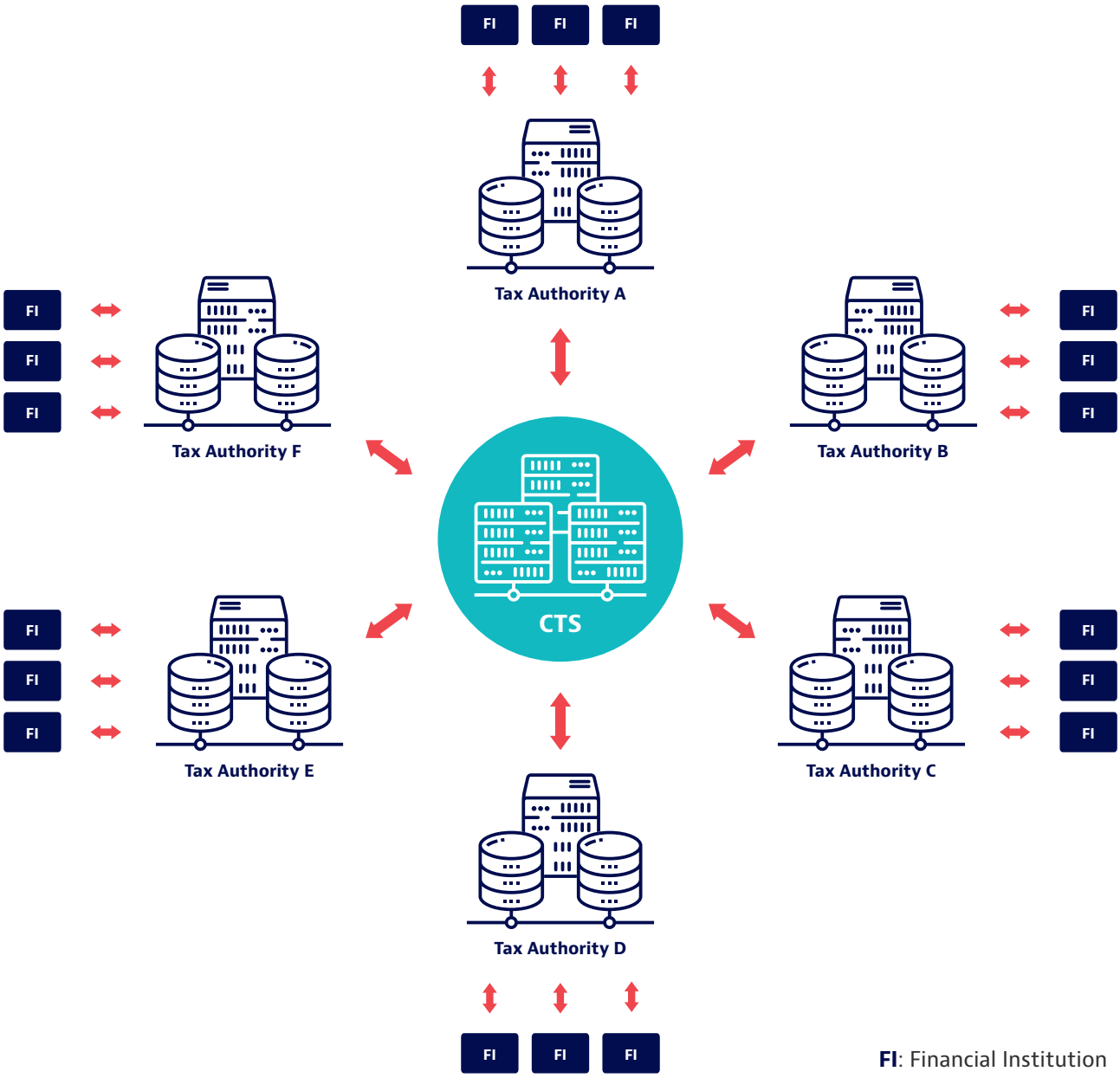
The CTS is a third-party technical solution that was developed on the request of FTA, which brings together the world's largest tax administrations. Its purpose is to ensure that the CRS information (and other tax information) can be exchanged in a highly secure and standardised manner.[76]

76. The CTS allows the exchange of additional types of tax information with enhanced functionalities, including the Authorised Transmissions feature. The Authorised Transmission feature requires competent authorities to pre-approve the sending and receiving of each message type for each partner jurisdiction before these exchanges can be made. This ensures only the correct message types are exchanged, in accordance with each competent authorities' legal and operational frameworks.

The Global Forum and a cross-OECD team (the CTS Secretariat) is responsible for the day-to-day running of the CTS, managing the provision of the CTS by the supplier and facilitating access to it by the tax administrations from its member jurisdictions. The security of the CTS is ensured through both the legal and operational framework put in place to deliver the CTS.

The CTS provides a secure and encrypted "pipe" through which Competent Authorities can bilaterally and securely exchange tax information with one another (see Figure 21).

FIGURE 21. **The Common Transmission System**

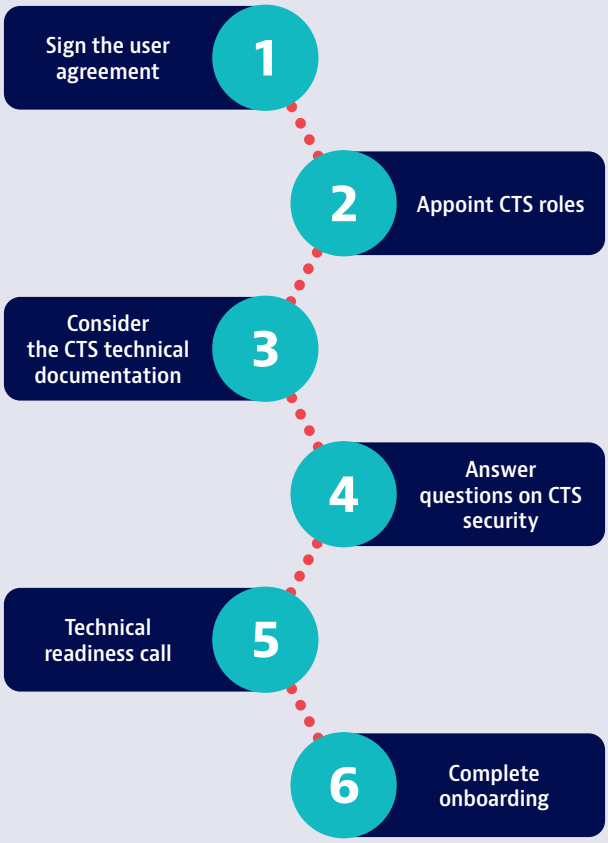


Only the intended recipient can access the files transmitted as they are encrypted by the sending jurisdiction prior to their transmission and can only be decrypted by the receiving tax authority following their receipt. Recognising that jurisdictions will have different systems to receive the data from Financial Institutions and to prepare the information for sending, the CTS offers competent authorities the ability to

Box 20. Joining the Common Transmission System

Once a jurisdiction is ready to join the CTS, it will contact the CTS Secretariat or its Global Forum Central Point of Contact to begin the process. The steps to join the CTS can be summarised as follows:

- **Step 1 – Sign the user agreement:** the CTS Secretariat will prepare a signature form for each jurisdiction which should be signed by the competent authority or by an authorised representative from the administration. The user agreement sets out the obligations of the jurisdiction in relation to the CTS, including security requirements and the requirement to pay user fees. The jurisdiction will become liable for annual user fees once they are in a position to begin using the CTS.
- **Step 2 – Appoint CTS roles:** the jurisdiction will inform the CTS Secretariat which individuals in their administration will perform key point of contact and administration roles for the CTS.
- **Step 3 – Consider the CTS technical documentation:** the CTS Secretariat will provide the jurisdiction's designated qualified personnel access to the CTS documentation. This includes technical specifications for connecting to the CTS and the file encryption requirements. From a technical perspective, it is key that jurisdictions intending to connect to the CTS via a server-to-server connection provide their IT-colleagues with the technical specifications as quickly as possible to allow them to undertake the necessary IT adaptations to be able to link up with the CTS.
- **Step 4 – Answer questions on CTS security:** the jurisdiction will be asked to provide detail on the security arrangements they will have in respect of access to the CTS.
- **Step 5 – Technical readiness call:** the CTS Secretariat will set up this call with the jurisdiction. The purpose of this call is to ensure that the jurisdiction is fully ready on a technical level to access the CTS.



- **Step 6 – Complete on-boarding:** once ready technically, and all other steps have been completed, the jurisdiction can link up with the CTS. This will first include access to the Conformance environment, for testing only, before being given access to Production (the live environment where real tax information is exchanged). Jurisdictions should note that access to Production will require the procurement of a security certificate from a limited list of authorised providers.

Full details on all steps will be provided by the CTS Secretariat following completion of Step 1.

access the CTS through a server-to-server link-up (SFTP), a browser-based manner (HTTPS), and through an API, in order to send and receive information. The CTS is not a database for the purpose of storing information.

Over 100 jurisdictions now use the CTS to securely exchange information under CRS, CbC Reporting and exchange of tax rulings standards. In early 2021, a major update to the system (CTS version 2.0) took place, allowing users to exchange over 25 forms of tax information through the CTS, including EOIR. Box 20 summarises the steps for joining the CTS.

Receiving CRS files

When a jurisdiction receives data, it must carry out similar steps as to when it is preparing files for sending. All sending jurisdictions will receive CRS Status Messages after they have sent a payload file, and reciprocal jurisdictions will of course receive payload files from their exchange partners. In both cases, the receiving jurisdiction will have to decrypt the file, and carry out a validation check on the information. The key steps jurisdictions need to carry out to receive files are:

- Receive files: this will be done through the agreed method of transmission (e.g. the CTS).
- Decrypt files: this will be based on the agreed method of encryption.
- Carry out a validation check on the file: this is to ensure that the file is in line with the relevant CRS XML schema requirements and that the data quality is in line with the requirements set out in the CRS Status Message User Guide.
- Send a CRS Status Message (only following receipt of a payload file).

CRS Status Messages

For each CRS payload file sent, the receiving jurisdiction will send a CRS Status Message to the sending jurisdiction indicating whether the file has been accepted or rejected and the outcomes of the validation checks carried out on the file and its records. The receiving competent authority should provide a Status Message response as soon as possible and no later than 15 days after the payload file was sent. Status Messages must be fully encrypted and will follow the same encryption standards as the sending of CRS payload files. Box 21 provides an example of exchanges between the sending and receiving partners.

Box 21. **Example for the sequence of exchanges under the CRS Status Message XML Schema**

In relation to an exchange of CRS information between Canada and France, the following events occur:

1 Canada sends a CRS message with new data to France
   - France is not able to decrypt the file and sends a CRS Status Message

2 Canada corrects the file with proper encryption
   - France found XML validation errors and sends a CRS Status Message

3 Canada corrects the XML validation issues and resubmits the file
   - France found no file error, but ten (minor) record errors. France accepts the file

4 Canada sends report with corrected data in respect of the ten record errors (the file contains only the ten corrected records)
   - France found no further errors. France accepts the file.

Source: CRS Status Message XML Schema: User Guide for Tax Administrations.

8. Ensuring effective use of the data

Strategies for effective use of data require the continuous development of new tools, skills and methodologies, moving from traditional data analysis to advanced analytics. The effective use of data through new technologies (advanced analytics, machine learning, and artificial intelligence) is highly dependent on organisational understanding of the impact of these new technologies on existing processes (compliance/audit/recovery) and requires strong partnerships between business users, data analysts and IT. Figure 22 depicts the key areas of the automatic exchange framework for an effective use of data.

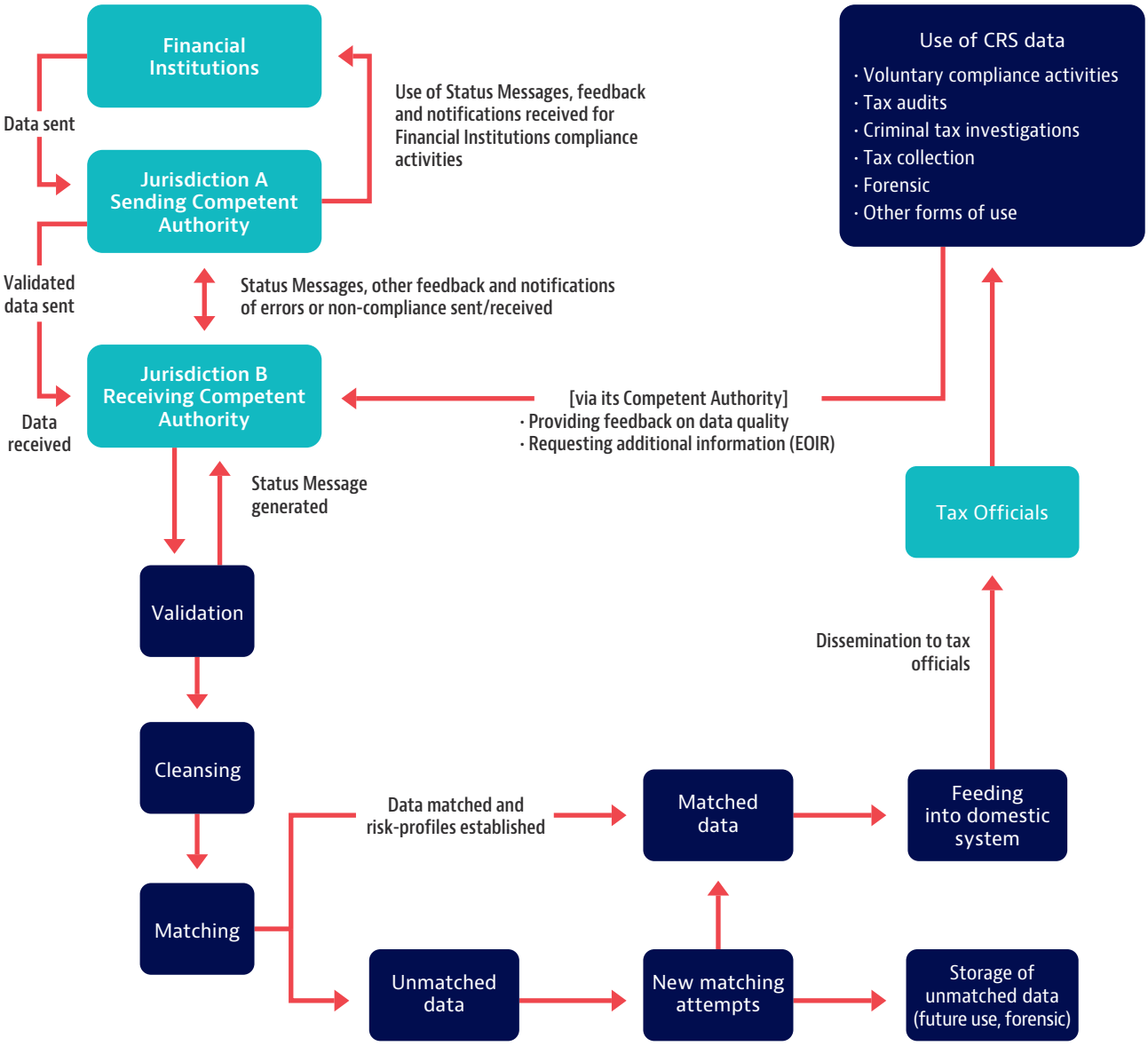
Every year in September, the competent authority of the receiving jurisdiction will receive CRS files in an XML format.

Prior to be uploaded in a national application, the receiving jurisdiction should do a technical check of the data file content using XML tools to make sure all "Validation" elements are present and if they are not, reject the file. This check includes the file validations set out in the XML Schema User guide (see Subsection 7.2.4 of the toolkit).

For the data received to be usable for domestic tax compliance purposes, it is essential to introduce the data into the national systems in such a way that it can be used effectively and accessed for tax compliance purposes.

The effective use of CRS data can be summarised in three different stages, illustrated in Figure 23. The first area covered is the treatment of the data (cleansing and parsing), in order to make the most efficient use of the data. Secondly, the matching of CRS data to domestic taxpayers using the identification information received (TIN, name, address, date of birth) is described in detail. Different matching possibilities are explored (automatic, fuzzy, manual matching) as well as what can be done with unmatched data. The third area considers the risk analysis to implement and the multi-pronged approach to consider in order to fine-tune the effective use of CRS data according to the different administrative frameworks or tax compliance strategies of the jurisdictions.

FIGURE 22. **Key areas of the AEOI framework for an effective use of data**

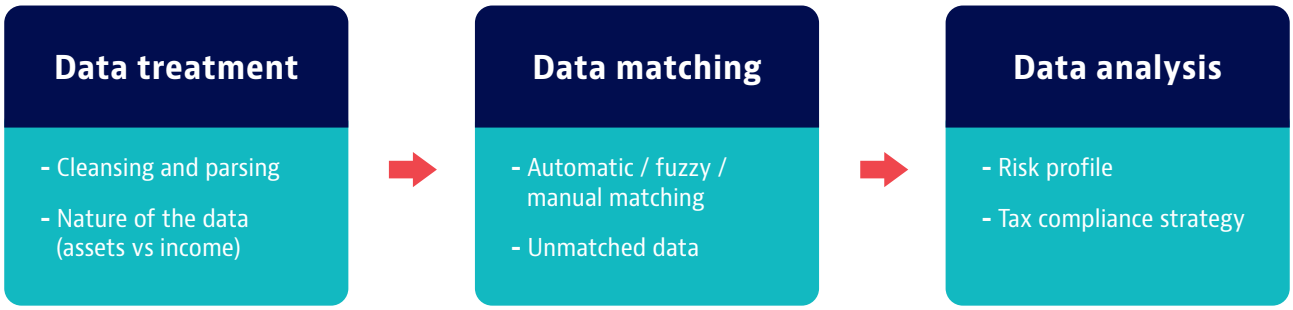


8.1. DATA TREATMENT

Although it is a Common Reporting Standard, the reporting of data can be done differently in practice, for instance with different structures to the names and addresses used. This makes data standardisation and cleansing very important.

Data cleansing involves identifying incomplete, incorrect, inaccurate or irrelevant parts of the data and then replacing, modifying or deleting the dirty or gross data. The process of data cleansing can include removing typographical errors or validating and correcting values against a known list of data. Some data cleansing solutions cleanse data by cross-checking with a validated data set. A common data cleansing practice is data parsing to make it into a format that is more readable and better for analysis. Data cleansing can also involve data harmonisation, which is the process of bringing together data from different file formats and transforming them into a coherent dataset (e.g. the expansion of abbreviations "st, rd" into "street, road"). Box 22 provides further examples of cleansing.

FIGURE 23. **Stages for an effective use of data**



Data cleansing can be done interactively with data processing tools (process of cleansing and unifying messy and complex data sets for easy access and analysis), or as a batch process using scripts (list of commands that are processed in sequence often without requiring user input or intervention).

After cleansing, the CRS dataset should be consistent with datasets in the domestic tax IT system. At this stage, the rules used to parse the data should be common to all data ingested into the domestic tax IT system. Fields are extracted from the CRS record in a fixed manner following the expected format of the data schema. Examples of common standards applied to all data in domestic tax IT system:

- text is uppercase
- multiple spaces are compressed to one space
- TINs follow expected pattern and length
- addresses are compared against domestic address structure.

Other rules can apply transformations to enable comparison of the data to other sources within the domestic IT system (for example, all currency figures are converted to national currency). Data cleansing differs from data validation in that validation almost invariably means that data is rejected from the system on entry and is performed at the time of entry, rather than on batches of data.

Box 22. **Examples of CRS data cleansing**

- Remove strings signifying missing values (NoFirstName / NoLastName / NA / NULL, etc.).
- String manipulation of names where a full name has been input into the Surname field.
- Pattern extraction for postcodes and dates of birth (some TINs appear to be dates of birth, others are Driver's licence numbers, which contain the DOB (date of birth) embedded in the value).
- Transliteration of errors for TINs and for postcodes (e.g. where a letter "O" has been captured instead of a number "0").
- Additional standardisation of Name Free and Address Free fields:
  - remove titles, special characters
  - where it is not possible to identify ordering of names, retain all possible combinations for matching, linked to a common ID
  - if both Address Free and a formatted address are provided, clean and retain both for matching.

8.1.1. Tax identification number

The TIN to be reported with respect to an account is the TIN assigned to the Account Holder (or its Controlling Persons where applicable) by its jurisdiction of residence (i.e. not by a jurisdiction of source).

However, TINs are not required to be reported with respect to Preexisting Accounts if:

i. it is not in the records of the Reporting Financial Institution

ii. there is not otherwise a requirement for the TIN to be collected by the Reporting Financial Institution under domestic law (subject to reasonable efforts to obtain the information).

As the TIN is the most unique identifier,[77] it is on this basis that automatic matching should be performed in the first instance. Therefore, the first data treatment should be the identification of data with a TIN and a check of its structure by the receiving jurisdiction against its own TIN's structure.

Because the TIN will not always be reported for Preexisting Accounts, it is important to have a matching process which uses other identifying information.

8.1.2. Other identification information

The name and the address are information required to be reported in relation to (i) Account Holders (Individual and Entity) that are Reportable Persons and (ii) Controlling Persons that are Reportable Persons. Additional information is also required to be reported in relation to Reportable Persons that are individuals, like the date or place of birth.

First and last name of Individuals

The first name is a data element required for CRS reporting (in the element FirstName). If the Reporting Financial Institution or tax administration transmitting the message does not have a complete first name for an individual Account Holder or Controlling Person, an initial or NFN ("No First Name") may be used instead.

The last name is a data element required for CRS reporting (in the element LastName). The Reporting Financial Institution or tax administration transmitting the message must provide the individual Account Holder's last name.

Name of entities

The element Name is one of the elements of the OrganisationParty_Type. This complex type identifies the name of an Account Holder that is an Entity as opposed to an Individual.

As a "Validation element", the legal name of the Entity that is reporting or being reported on must be reported by Financial Institutions.

Address

There are two options for the address type in the CRS schema – AddressFix and AddressFree. AddressFix should be used for all CRS reporting unless the Reporting Financial Institution or tax administration transmitting the message cannot define the various parts of the Reportable Person's address. The "City" data element is the only one required for schema validation. All other data elements are optional (street, postcode, building identifier…).

Date of birth

The date of birth is not required to be reported with respect to Preexisting Accounts if:

i. it is not in the records of the Reporting Financial Institution

ii. there is not otherwise a requirement for the date of birth to be collected by the Reporting Financial Institution under domestic law (subject to reasonable efforts to obtain the information).

Place of birth

The place of birth is not required to be reported for both Preexisting and New Accounts unless the Reporting Financial Institution is otherwise required to obtain and report it under domestic law and it is available in the electronically searchable data maintained by the Reporting Financial Institution.

8.1.3. Domestic databases

Before the cleansing and parsing process, it is essential to identify the domestic databases (public and private) that will be used for matching the data. Examples of domestic databases are provided in Box 23.

This mapping exercise identifies the data to be used and matched (TIN, first and last name, address, date and place of birth). Once these domestic databases are identified, it is necessary to analyse their structure in order to know what cleansing and parsing work is needed to enable automatic matching:

- use of upper or lower case letters (e.g. Paris or PARIS)

77. A section of the AEOI portal provides an overview of domestic rules governing the issuance, structure, use and validity of TIN or their functional equivalents: www.oecd.org/tax/automatic-exchange/crs-implementation-and-assistance/tax-identification-numbers.

- date of birth format (in the CRS XML schema the data format is YYYY-MM-DD)
- address structure (separation of building, street, postcode, city) or aggregation of information. Depending on jurisdiction or Financial Institution, the data may be across a number of boxes and may be in a different order to that expected by data systems (Figure 24 provides an example).
- separation of first name and surname.

8.1.4. Cleansing and parsing process

The errors and inconsistencies to be corrected include variations in address formats, use of abbreviations, misspellings, outdated information, inconsistent data, and names with transposition errors. The cleansing and parsing process fixes these errors and inconsistencies by:

- parsing the name and address input data into individual elements
- removing all characters which are not a space, letters A-Z, or numbers 0-9
- standardising name and address data, using standardised versions of nicknames and business names and standard abbreviations of address components, as approved by the postal service or used by the tax database.
- correcting address information such as street names and city names.

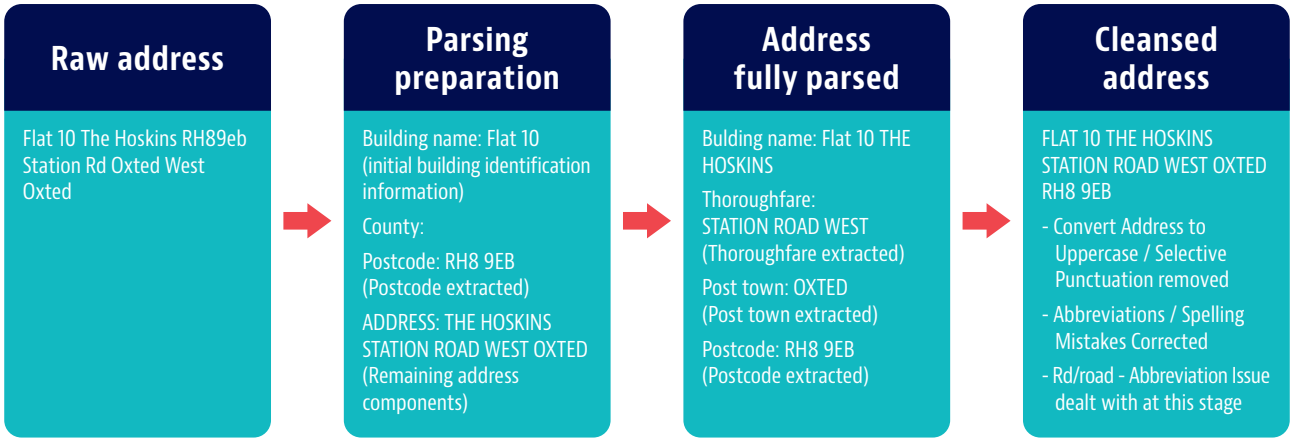
Box 23. **Domestic databases**

Some jurisdictions maintain an incomes register or similar which is a centralised national database for information on individuals' income. It contains comprehensive data on earned income, pensions and benefits. All employers and all payers of benefits are obligated to report information on incomes paid out to the incomes register in real time. The data can be used by the tax administration, the social insurance institution, the unemployment insurance fund as well as earnings-related pension providers.

Other jurisdictions have a national population register with high quality information on all national inhabitants and persons immigrating to the jurisdiction. The quality of the national population register is a decisive factor for a high matching rate. The register contains updated information on the inhabitants names, addresses, family relations, civil status and the history of name and address changes.

- extracting postal codes from the address free-text field.
- augmenting names and addresses with additional data such as gender, postal code, country code, apartment identification.
- identifying dates of birth that may have been submitted in the incorrect format (MM/DD/YYYY).

FIGURE 24. **Address cleansing**



Data cleansing software systematically searches for discrepancies or anomalies by using algorithms or lookup tables. It then corrects the issues. An automated process of this kind is much more efficient than trying to fix errors by hand.

Data cleansing tools generally contain these and other similar feature sets:

- raw data ingestion
- support for a wide variety of data formats (e.g. .csv, .xml…)
- phone and email validation
- address and postal code cleansing
- automatic or manual data mapping
- data consolidation and ETL (Extract, Transform, Load)
- sample testing
- data validation, matching, reconciliation
- data analysis, charting.

An example of cleansing and parsing is provided in Box 24.

Simple data cleansing tools are open source and available for free. Alternatively, vendors offering business intelligence or data management tools also provide data cleansing tools. Such data cleansing tools are available on a subscription basis. Pricing corresponds to volume of data stored or exported. Pricing may also correspond with the number of validations (e.g. email, address) performed.

It is clear that building on experience of cleansing helps to reduce the heterogeneity in the matching for the future exchanges and allow a possible reattempt of matching of previous received CRS data.

Any modification made during this process should be well documented so that future users can identify and repeat the original process. The data should be kept in its original format throughout the process.

8.1.5. Nature of CRS data

The use of CRS data will be specific to each jurisdiction's domestic tax framework and context. Some jurisdictions will only tax incomes while other jurisdictions may also impose taxes on the value of the assets. Data treatment should consider the linkage with all relevant taxes (e.g. income tax, wealth tax). CRS data include asset and income information (see Table 25).

For the income, different codes exist to identify the payment type:

- CRS501 = Dividends
- CRS502 = Interest
- CRS503 = Gross Proceeds/Redemptions
- CRS504 = Other – CRS. (Example: other income generated with respect to the assets held in the account).

For an effective use of CRS data, it is important to consider the classification of income and assets between the CRS and the domestic tax legislation, in order to identify what tax treatment should be implemented (e.g. the account balance can be included for the wealth tax, a dividend can be taxed at the lower long-term capital gains tax rate instead of at the higher tax rate used on an individual's regular income).

Nevertheless, jurisdictions should consider that the underlying asset itself (the account balance or value) will often be linked to previous years' income. This is particularly relevant in the first year of reporting when the account is brought to the attention of the tax authority for the first time. For example, if a taxpayer undeclared income in previous years and placed this income in an offshore account, this income will be reflected in the value of the account balance alongside any interest accrued until the reporting year.

The data treatment should also consider possible discrepancies between CRS data and data included in tax returns (e.g. difference between CRS reporting periods and domestic tax years, CRS data from joint accounts where each account holder has the total balance and payment to the account reported, negative balances).

Box 24. **Cleansing and Parsing example**

Example input

The data contains a nickname, a last name, and part of a mailing address, but it lacks the taxpayer's full name, complete street address, and the state in which he lives.

NAME	STREET ADDRESS	CITY	ZIP CODE
Joe Doe	8500 Vermilion Lake Suite 710	Peyla	55790

Process

The mapping process can use a Name and Address operator to cleanse name and address records, followed by a Splitter operator to load the records into separate targets depending on whether they were successfully parsed.

In the Mapping Editor, the following operators should be used:

- A CRS data table from which you extract the records. This is the data source.
- A Name and Address operator. This action starts the Name and Address Wizard which is a user interface that presents a sequence of dialog boxes that lead the user through a series of well-defined steps.
- A Splitter operator.
- Three target operators into which you load the successfully parsed records, the records with parsing errors, and the records whose addresses are parsed but not found in the postal matching software.

The general steps required to design such a mapping and make the listed changes to the sample record are:

1) Map the attributes from the CRS data table to the Name and Address operator. Map the attributes from the Name and Address operator outgroup to the Splitter operator.
2) Define the split conditions for each of the outputs in the Splitter operator and map the outputs to the targets (successfully parsed records, records with parsing errors, and the records whose addresses are parsed but not found).

Example output

In this example, the following changes were made to the input data:

- All letters were capitalised.
- Joe Doe was separated into separate columns for FirstName and LastName.
- Joe was standardised into JOSEPH and Suite was standardised into STE.
- Vermilion Lake was corrected to VERMILION LAKE BLVD.
- The first portion of the postal code, 55790, was augmented with the ZIP+4 code to read 55790-3813.

FirstName	LastName	Street	SuiteIdentifier	City	PostCode
JOSEPH	DOE	8500 VERMILION LAKE BLVD	STE 710	PEYLA	55790-3813

Table 25. **Asset and income information in CRS data**

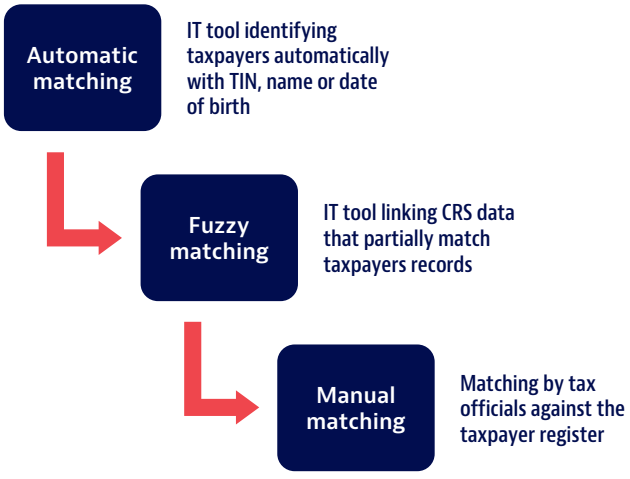
Type of Financial Account	Asset	Income / gains
Depository Account	The account balance or value	The aggregate gross amount of interest paid or credited to the account during the calendar year
Custodial Account	The account balance or value	• The aggregate gross amount of dividends paid or credited to the account during the calendar year (or relevant reporting period) • The aggregate gross amount of interest paid or credited to the account during the calendar year (or relevant reporting period) • The gross proceeds from the sale or redemption of property paid or credited to the account during the calendar year (or relevant reporting period) with respect to which the Financial Institution acted as a custodian, broker, nominee, or otherwise as an agent for the Account Holder • The aggregate gross amount of all other income paid or credited to the account during the calendar year (or relevant reporting period).
Equity and debt interest in certain Investment Entities	The value of the debt or equity interest that the Account Holder has in the Financial Institution.	The aggregate gross amount of payments paid or credited to the account during the calendar year (or relevant reporting period), including redemption payments.
Cash Value Insurance Contract and Annuity Contract	The Cash Value of the Insurance Contract or Annuity Contract.	The aggregate gross amount of payments paid or credited to the account during the calendar year (or relevant reporting period), including redemption payments.

8.2. DATA MATCHING

Data matching (also known as record or data linkage, entity resolution, object identification, or field matching) is the task of identifying, matching and merging records that correspond to the same Individuals or Entities from several databases. Based on different technologies including applied statistics, data mining, machine learning, artificial intelligence, database management, and digital libraries, several processes, depicted in Figure 25, exist to improve the accuracy of data matching:

- Automatic matching usually makes use of search keys that run algorithms based on combinations of fields (TIN, name, address for instance).
- Fuzzy matching allows approximate matches (with approximations made for the received data, such as similar names or addresses).

FIGURE 25. **Matching process**



- Manual matching is often applied to unmatched data and relies on a simpler range of search keys (e.g. address only) or comparisons with other external databases.

8.2.1. Automatic matching

The first step in the matching process is usually automatic matching, starting with the matching of TINs. Thereafter, multiple iterations of the automatic data matching process based on, for instance, name, address, date of birth, International Bank Account Number can be implemented.

Even when a match with a TIN is made, it is recommended that the quality of this match be checked against other identifying data.

Tax authorities have access to a wide spectrum of methodologies and they have the potential to rapidly develop and integrate new ones. Different record-linkage software packages exist.[78]

A highly scalable full-text search and analytics engine is recommended and the software should be able to store, search, and analyse big volumes of data quickly and in near real time.

In addition, the use of an advanced matching software that "learns" from previous sets of matches should be considered. This software should be able to recall previous matches (e.g. where a bank account was successfully reconciled in Y 0 but not in Y 1, the reconciliation software must be able to remember previous matches, to detect and highlight the initial match).

Phase 1 – Automatic matching with a TIN

The TIN of the received record is compared with a domestic register containing similar information, such as the taxpayer register, the legal entities register, the foreign accounts register (if any) and the tax residency database (if any). The national TIN is checked and the record is given a status indicating that it has been matched with a valid national TIN.

78. Different record-linkage software packages exist such as the "SAS (PVS) Matcher®", "BigMatch®", "d-blink®" and "MAMBA®". Tax administrations can also have an easy access to open-source packages, such as "fastLink®", "RecordLinkage in R®", "Apache Spark®", "Python®", "PostgreSQL®", "ElasticSearch®".

Phase 2: Automatic matching without a TIN

If the record does not contain a valid national TIN, other data elements shall be used for the matching. Combinations of name, date of birth and address can be used to get a unique match.

Based on the experience, the best combinations are, in order of reliability:

i. name and date of birth;

ii. name, street name and postcode;

iii. name, city and street name.

8.2.2. Fuzzy matching

Fuzzy Matching is a technique that helps identify two elements of text, strings, or entries that are approximately similar but are not exactly the same. It works with matches that may be less than 100% perfect when finding correspondences between CRS data and entries in a domestic database. An example with the name matching is provided in Table 26.

Where the matching rate is 100% with automatic matching, a lower confidence match can be used with fuzzy matching. It is necessary to assess the confidence of the match made between the CRS data and taxpayer records, as this may determine suitable use of the data.

Figure 26 provides an example of match quality score. In general, a high-confidence match is better achieved with the TIN and date of birth (does not change) than with address and postcode (likely to change). Date of birth is a very strong key as this doesn't change and is particularly important for records where a TIN is not provided. Both date of birth and TIN also lend themselves well to extraction and comparison as the formats are known. Regular expressions are employed in the matching, as this allows for easy removal of optional or special characters and delimiters.

If a record is matched during the fuzzy matching stage, the IT solution should allow a record with similar information for a given set of the data elements to be automatically matched when received in a future transmission.

FIGURE 26. **Example of Match Quality Score**

Data matched	Match Score	Useable Match
TIN, First Name, Surname, Address, Date of birth	100%	Yes
TIN and Name, Surname	95%	Yes
First Name, Surname, Address, Date of birth	81%	Yes
Surname, Address	30%	No

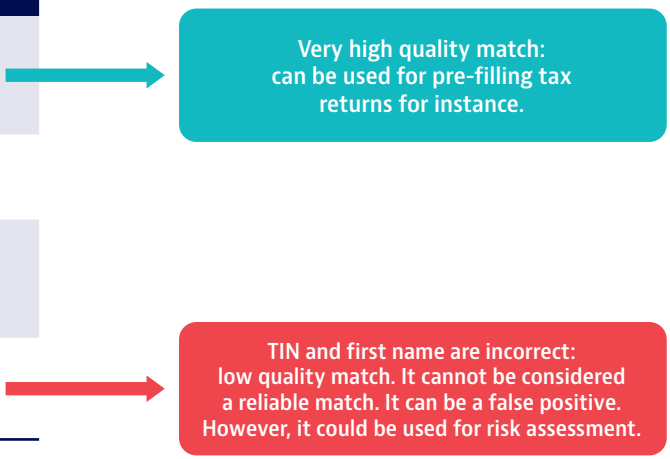


Table 26. **Challenges of Name matching**

Challenge	Example
Missing Spaces & Hyphens	MaryAnn ↔ Mary Ann ↔ Mary-Ann
Missing Components	Phillip Peter Corr ↔ Phillip Corr
Split Database Fields	Dick. Van Dyke ↔ Dick Van. Dyke
Spelling Differences	Abdul Rasheed ↔ Abd al-Rashid
Titles & Honorifics	Dr. ↔ Mr. ↔ Ph.D.
Out-of-Order Components	Diaz, Carlos Alfonzo ↔ Carlos Alfonzo Diaz
Multiple Languages	Mao Zedong ↔ Мао Цзэдун ↔ 毛泽东
Nicknames	William ↔ Will ↔ Bill ↔ Billy
Truncated Components	McDonalds ↔ McDonald ↔ McD
Initials	J.J. Smith ↔ James Earl Smith
Similar Names	Eagle Pharmaceuticals, Inc. ↔ Eagle Drugs, Co.

Different methods exist and can be implemented. Hybrid approaches fill the weaknesses of one approach with the strength of another:

Common key methods

The principle of these methods is to reduce strings to a key based on their pronunciation or linguistic semantics. These methods use phonetic algorithms which turn similar sounding names into the same key, thus identifying similar names.

- The Metaphone algorithm returns a coded value based on the English pronunciation of a given word. The coded value for the names John and Jan would return the value JN for both names.
- The Double Metaphone algorithm can return a primary and secondary encoded value for a string. The names John and Jan each return Metaphone key values of JN and AN.

- The SoundEx algorithm returns a single coded value for a name which consists of a letter followed by three digits. The letter is the first letter of the name, and the numbers encode the remaining consonants. An example is provided in Box 25.

- The refined SoundEx algorithm is six digits long, the initial character is encoded, and several possible encodings can be returned for a single name. Using this algorithm, the name John returns the values 160 000 and 460 000, as does the name Jan.

Edit distance methods

Edit distance is a way of quantifying how dissimilar two strings (e.g. words) are to one another by counting the minimum number of operations required to transform one string into the other. “Cindy” and “Cyndi” have an edit distance of 1 since the “i” and “y” are merely transposed, whereas “Catherine” and “Katharine” have an edit distance of 2 as the “C” turns into a “K” and the first “e” becomes an “a”. The approach of the algorithms that belong to this method is to look at how many character changes (number of insertions, deletions or transpositions of characters) are needed to move from one name to another:

- The Levenshtein algorithm calculates the distance between two strings by looking at how many edit steps are needed to get from one string to another. The score indicates the minimum number of changes needed. For instance, the difference between John and Jan would be two; to turn the name John into Jan you need one step to replace the O with an A, and another step to delete the H.

- The Jaro Winkler algorithm calculates a similarity index between two strings. The result is a fraction between zero, indicating no similarity, and one, indicating an identical match (e.g. s1 = “CRATE”, s2 = “TRACE”; Jaro Similarity = 0.733333).

8.2.3. Manual matching

Manual data matching involves visually checking CRS data against the taxpayer register. There may be cost implications for both staff resources and the time it takes to deal with large volumes of data. However, manual data matching allows tax officials to interpret and make a judgement on complex data which may achieve a more accurate result.

Box 25. **Example of SoundEx algorithm**

The formula for turning a word into a SoundEx code consists of a letter followed by three numbers: the letter is the first letter of the word, and the numbers assign a code to the remaining consonants.

The SoundEx code can be obtained in the following way:

1) Keep the first letter of the name and delete all other occurrences of a, e, i, o, u, y, h, w.

2) Replace the consonants with numbers as follows (after the first letter):

   b, f, p, v → 1

   c, g, j, k, q, s, x, z → 2

   d, t → 3

   l → 4

   m, n → 5

   r → 6

3) If two or more letters with the same number are adjacent in the original name (before step 1), keep only the first letter.

Using this algorithm, "Robert" and "Rupert" both return the same string "R163", while "Rubin" gives "R150".

Any data not matched in the course of the automatic or fuzzy matching procedure should be further treated manually. If record pairs are classified into potential matches, a manual matching process is needed to decide their final match status (matched or non-matched).

The manual matching process can be organised in different ways, depending on where the data eligible for manual identification is stored or the availability of human resource to perform manual identification.

For manual matching, software can be developed to present suggestions for possible taxpayers from the domestic taxpayer database and a search field if the suggestion list of taxpayers does not contain the correct account holder. The user interface for manual matching should offer search criteria that enable filtering of the records the tax administration wants to match manually

in line with its compliance activities (e.g. compliance activity and campaigns may focus on certain tax jurisdictions, income types, records with account balances above a certain threshold (high net worth individuals (HNWI)). The searched records should be available in a list for selection by tax officials. Figure 27 provides an example of a user-interface.

The conclusion made by the tax official should be recorded:

- in case of a manual match, the national TIN is assigned to the appropriate record
- when a record cannot be identified manually, the reason which prevents to perform the manual identification should be indicated.

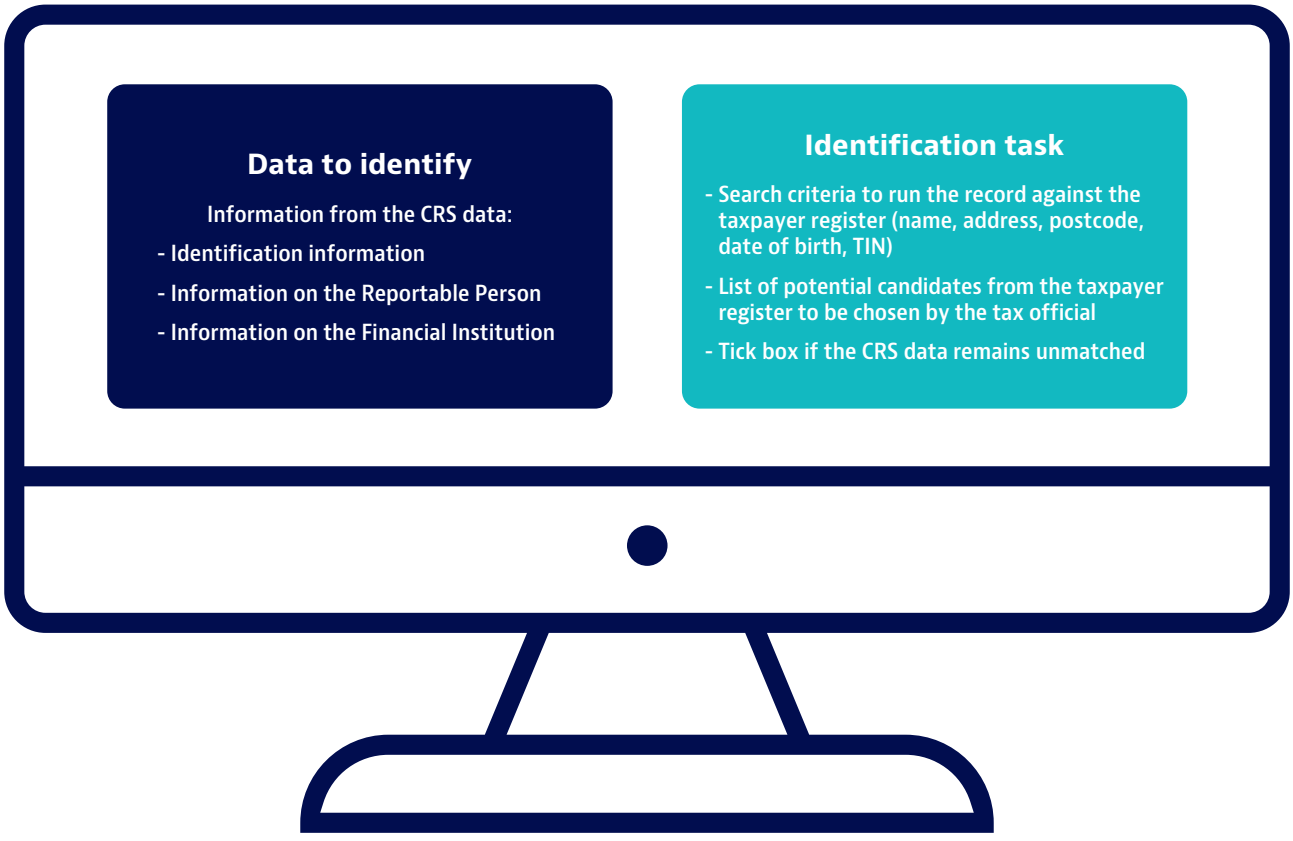
The result of the manual matching shall feed the automatic matching process in order to improve it for the future exchanges. If a record is manually matched, a record with similar information for a given set of the information elements should be automatically matched when received in a future transmission. Results from the automatic, fuzzy and manual matching should be indexed with the taxpayer register. These indexes are used for searching/matching based on taxpayer's TIN or a combination of name, date of birth and address.

8.2.4. Unmatched data

After applying manual matching procedures, some CRS data sets received will still not be able to be matched to a particular taxpayer. This unmatched data should be stored for future use or reattempt. This unmatched data can be reused in subsequent years, and thus benefit from enriched data in future exchanges, improved data matching techniques or wider third party databases. Where the tax authority determines that it does not need the data, it should be destroyed.

It is good practice to provide your partner with feedback on the information reported, particularly if there is a Reporting Financial Institution in their jurisdiction which reported an above average number of accounts which could not be matched.

FIGURE 27. **Example of user interface for manual matching**



Receiving jurisdictions can also carry out a risk analysis on any unmatched data to identify patterns and trends, such as:

- any connection between unmatched records and a particular Financial Institution or a particular partner jurisdiction which may indicate non-compliance with the CRS.
- taxpayers potentially falsely declaring identifying information or tax residency to avoid reporting.

When CRS data related to a High Value Account is unmatched and where appropriate, a jurisdiction may consider seeking more information from the sending partner through an EOI request specifying the CRS-AEOI reference and explaining the unsuccessful investigations carried out. The reason for the exchange (such as any indicia based reason) could be requested.

8.3. DATA ANALYSIS

Once CRS data is matched, it has a number of potential uses : improving compliance and customer service by pre-populating more asset or income-related fields within a tax return; deterring taxpayers from engaging in tax evasion practices through mass and targeted communication building on CRS data; mapping the financial interests and cross-border operations of taxpayers; securing international debt collection activities; improving cooperation with other governmental agencies, especially those that are in charge of the fight against money-laundering; etc.

8.3.1. Risk analysis

Using CRS data to identify tax evasion, tax authorities can tackle a wide range of non-compliance behaviours in a proactive, targeted and cost-effective manner. This requires knowledge in three main areas:

- information technology skills to develop the data collection and interrogation systems
- statistical and analytical skills to develop the algorithms and models
- tax expertise to ask the right questions, interpret the results and make more informed risk-based decisions. This experience should include offshore/international tax expertise in order to understand the tax risks associated with different financial accounts, entity structures (e.g. trusts) and the significance of certain information reported (e.g. account balances and income).

Tax authorities should analyse and consolidate the CRS data with other available tax data to establish the risk profile of taxpayers. One useful and relevant source of information can be any VDP that has been put in place. A basic check would review the comprehensive tax situation of a taxpayer to verify if whether all foreign bank accounts, assets and related income have correctly been disclosed. High-risk taxpayers will typically require more in-depth investigation and checks due to the complexity of their affairs, while medium/low-risk taxpayers will often require fewer control interventions.

Organisation

To achieve their strategy, the tax authorities have to choose the most appropriate analytical operating model:

- A centralised model, with a central analytical function supporting the rest of the business. A centralised model encourages collaboration within the analytics team and allows for better supervision of analytical activities and close quality control. However, there is a risk of creating organisational silos between the analytics team and the business units that use the analytical data.
- A decentralised model, with teams of analysts integrated or co-located in specific business units. Analysts can better understand the language of the business, as well as the technical subject matter. However, there is a risk of sub-optimal coordination and knowledge sharing, leading to duplication, fragmentation or missed opportunities.
- A mixed approach where tax administrations seek the benefits of each model: a central team that provides leadership, coordination and empowerment for analysis, combined with close integration of analysis professionals in the business units.

Whichever organisational structure is in place, tax authorities need good information on the HNWI segment and should have processes in place to access existing information held on HNWIs effectively. Jurisdictions often have a dedicated HNWI unit in place. Such a unit will typically take responsibility for those taxes that have a direct impact on the HNWI's personal tax liabilities. In some countries the coverage extends further to dealing with associated investment and business entities such as trusts, controlled investment companies and other operating entities.

Technical aspects

With cleansed CRS data, machine learning and artificial intelligence can make increasingly accurate decisions, and when combined with the processes of robotic process automation, tax administrations can achieve efficient analytics.

- Robotic process automation (RPA) is an application that performs highly logical automated tasks. RPA acts as a software engineered to recognise humans' workflow patterns, handle ruled-based processes, and, ultimately, automate manual work.
- Machine learning is the science of teaching computers to gradually improve their performance in a given task. Unlike RPA, which is logical and condition-based, machine learning requires the computer to have some degree of cognitive ability. Machine learning can process and learn data by pattern recognition in massive data sets on its own, without the constant supervision of programmers.
- Artificial intelligence refers to computer systems that can perform human-like tasks. It is not about learning, but about creating a neural network that absorbs large amounts of data and, by itself, builds algorithms that help it determine the right way to perform a task.

Some examples of technical data analytics are provided in Box 26. When the data is used after the risk analysis, if the tax auditor considers the risk level attached to the file to be incorrect or finds that the CRS data is incorrect, the tax auditor should be given the opportunity to revise the risk level or provide feedback to the unit responsible for determining the risk level. This feedback is essential for improving the efficiency of data analytics like machine learning or artificial intelligence.

Box 26. **Use of data – Technical examples**

Robotic process automation

Using this type of tax robotics, a tax administration can program a computer to go to certain internal or external websites to run tasks. For example, it is possible to automate the process to open a spreadsheet with CRS data, to select some data (e.g. TIN or name, amount of interests), to open an internal database to consult the taxpayer's file and to crosscheck the amount of interests from the CRS data with the amount of interests declared in a tax return. RPA will then mimic the tax auditor's actions of clicking on buttons and setting up filters, and generate a report for the tax auditor.

Machine learning

Innovative algorithms[79] help to predict linkages between bank account references and individuals, compute social network metrics, and traverse relationships with several degrees of separation. As a result, the tax administration is able to identify networks of unusual behaviours which would not be easy to identify manually. Furthermore, machine learning tax algorithms can be developed to search for and identify assets linked to certain bank accounts, based on historical classifications.

For instance, anomaly detection is a form of unsupervised learning, which takes a large data set and searches for outliers and anomalous data which differs significantly from the rest of the data set. Algorithms will report back not just which entries are anomalous, but provide scoring on the extent to which they lay outside the rest of the data set (e.g. account balance in comparison to the declared income or the date of birth).

Artificial intelligence

Referred to as "predictive modelling," artificial intelligence applications are now being used by tax administrations to identify cases having characteristics that could indicate potential fraud. It often helps find subtle clues hidden in mounds of data that are sometimes missed or overlooked by tax auditors.

For instance, a computer is supplied with training data, such as a set of CRS data with the classification decisions already made – for example identifying whether a category of income is taxable or not. An algorithm then "learns" what makes these entries unique and uses this logic to analyse future activities. When combined with natural language processing artificial intelligence, the system can review income declared in CRS data to determine which category of income is taxable at normal or special rates.

79. The main open source tools used are Neo4J®, Gephi®, R®, and Java® (for algorithm development).

8.3.2. Reviewing taxpayer compliance

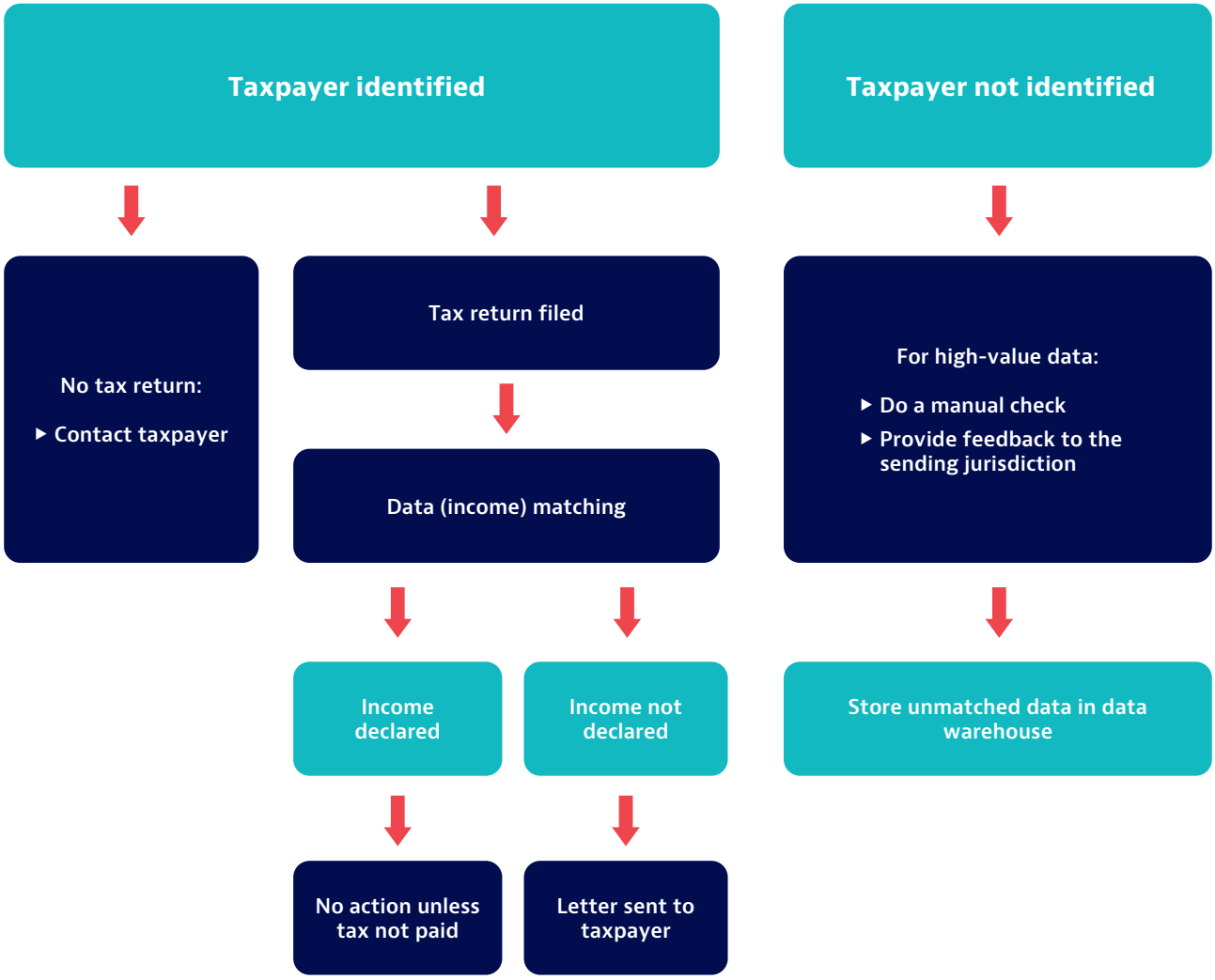
After the different stages of data treatment and analysis, tax authorities can use the CRS data to carry out compliance activities.

At first, it is important to define a compliance strategy relying on four different blocks:

- segmentation as a way to prioritise resources where high risk could be expected. Segmentation can be determined by value/amount, jurisdiction, type of Financial Institution, etc.
- immediate use by assessment of CRS data in audits, supporting compliance to prompt taxpayer behaviours (e.g. nudge letters, pre-filling of returns), or information and education (website, informative letters)
- gaining perspective by mapping asset locations, identifying networks, understanding the scale of assets and developing predictive and behavioural models
- measuring the effectiveness from increases in tax collection through amended tax returns and penalties and interests, statistics on declared financial income, voluntary disclosures and yield from interventions prompted directly by CRS data or successful prosecution of criminal activity.

An example of compliance strategy is illustrated in Figure 28.

FIGURE 28. **Example of a basic compliance strategy**



This compliance strategy can consider different timeframes by assessing past or current non-compliance of taxpayers on the one hand, and future non-compliance by predicting taxpayer behaviour or revenue losses on the other hand.

Past or current non-compliance

The first use of CRS data by a tax authority is to check whether the CRS data received is correctly reported by the taxpayers in their tax returns (e.g. account balance or income to be reported in an income or wealth tax return). Depending on the amount of CRS data they have received and the discrepancies found, tax authorities may adopt different strategies:

- No discrepancy: no need to open a case.
- In case of discrepancy: a compliance strategy should be tailored and implemented.
  - A risk profiling system would select a defined number of cases for review, based on the discrepancies. This case selection system will typically take into account factors such as reported income, taxpayer risk ratings, past compliance behaviour in terms of accuracy and timeliness.
  - Depending on the amount of the discrepancy, different compliance approaches should be considered. For instance, the tax administration could consider sending letters (e.g. a discrepancy letter) for low/medium-value discrepancies, and specific follow-up actions (e.g. desk or on-site audit) for high-value discrepancies.
  - For this compliance check to take place, the tax administration will need to make the matched data available to the tax auditors. This can be done by transferring the data to the relevant tax auditors or by including the matched data in a centralised database which tax auditors can access.
  - The audit of tax returns against the data received from CRS-AEOI could be done on a systematic basis, or could be done on a sample basis. Any sample check could be random or based on prior risk profiling to select returns on the basis of the amount of the discrepancies.

There are areas where the Standard provides optional provisions (see Section 6.3 of the toolkit) which are typically intended to provide greater flexibility for their Financial Institutions in carrying out their due diligence and reporting and therefore reduce their costs. But at the same time, it results in some differences in the CRS data which tax auditors should be aware of. These differences alongside other key points tax auditors should be aware of when interpreting the data are listed in Box 27.

Some of the different procedures available to follow up with the taxpayer directly in cases of discrepancy are:

- Nudge letters indicating that the tax administration has received information that the taxpayer may have offshore income or assets, and inviting the taxpayer to correct its tax return should there be errors in what has been reported. An example of nudge letter is provided in Box 28.
- Discrepancy letters are notices stating that there appears to be a discrepancy or error within an individual's tax return and it will be assessed unless petitioned. The taxpayer has a time limit to respond, otherwise the discrepancies can result in a tax assessment.
- Tax audits including desk audits (the tax auditor normally requests specific documentation to support particular items on the tax return by mail) and on-site audits (the tax auditor performs the audit at the premises).

CRS data can also be used for further compliance strategies, such as:

- Anomaly detection techniques which highlight relationships, behaviours and events that deviate from the norm. They are a means of identifying potential new fraud and compliance risks. Techniques such as statistical outlier detection and cluster analysis can uncover anomalies in taxpayer behaviour and circumstances. Clustering algorithms seek to group data points together to identify entries with common features (e.g. same address or same financial institution). Unlike a more traditional two dimensional scatter graph, clustering algorithms work well with more than two variables and can also identify which variables give rise to the most anomalies in the data. Anomaly detection can also look at changes over time to identify a deviation from a historical pattern, which may indicate fraud. The "nearest neighbour" approach is commonly used to compare a taxpayer's return with those of his peers to identify outliers or unusual cases for further investigation.

- Social network analysis which uncovers hidden or unexpected relationships that indicate collusion between suspicious groups or organised fraud rings. It relies on linking entities in the data (e.g. individuals, businesses, mobile phone numbers and bank accounts) using transactional information, such as bank account references collected during criminal investigations, to identify potential criminality in networks of individuals and businesses.

Box 27. **Use of data – Points of attention for tax auditors**

In relation to income and assets reported

Differences can exist due to the optional provisions possible under the CRS.

- Gross proceeds: this option phases in the requirement on Reporting Financial Institutions to report gross proceeds, but does not apply to exchanges under the CRS MCAA. The idea behind the option to report gross proceeds in a later year was introduced to allow Reporting Financial Institutions to have additional time to implement systems and procedures to capture gross proceeds for the sale or redemption of Financial Assets.
- Calculation method for balances: alternative approach to calculating account balances. A jurisdiction that already requires Financial Institutions to report the average balance or value of the account may allow average balances or values to be reported instead of the account balance or value as of the end of the calendar year or other reporting period. The end of year balance is the amount to be reported but the amount will be different if the average balance is instead reported in the CRS data.
- Reporting periods: use of other reporting period. A jurisdiction that already requires Financial Institutions to report information based on a designated reporting period other than the calendar year may wish to provide for the reporting based on such reporting period. The reporting period for CRS-AEOI may therefore differ from the receiving jurisdiction's fiscal year.
- Negative balances: an account with a balance or value that is negative must be reported as having an account balance or value equal to zero. As negative balances can be used for the determination of the net worth, the CRS zero value can be misinterpreted.

In relation to Account Holders and Controlling Persons reported

The following are points of attention for tax auditors which are relevant to all CRS information (and not based on any particular optional provision):

- Preexisting Account due diligence on the basis of indicia: for Preexisting Accounts, the jurisdiction of residence is based on the residence address test or the indicia search (or a self-certification if obtained).
- Determination of Controlling Persons on the basis of AML/KYC: when the Account Holder is a Passive NFE, the Reporting Financial Institution must determine whether the Passive NFE has Controlling Persons by reviewing the AML/KYC documentation it has available with respect to the Account Holder. The type of control reported should also be taken into consideration (e.g. ownership, other means, senior managing official for legal persons).
- Settlor, protectors, trustee and beneficiaries of trusts: if a settlor, beneficiary or other person exercising ultimate effective control over the trust is itself an Entity, that Entity must be looked through (including any further intermediate Entities), and the ultimate natural controlling person(s) behind that Entity must be treated as the Equity Interest holder.
- Joint accounts: each holder of a jointly held account is attributed the entire balance or value of the joint account, as well as the full amounts paid or credited to the joint account.
- Attribution of full balance/value and income to each Controlling Person: each holder is attributed the entire balance or value for:
  - an account held by a Passive NFE with more than one Controlling Person that is a Reportable Person
  - an account held by an Account Holder that is a Reportable Person (or a Passive NFE with a Reportable Controlling Person) and is identified as having more than one jurisdiction of residence
  - an account held by a Passive NFE that is a Reportable Person with a Controlling Person that is a Reportable Person.

Box 28. **Use of CRS data – Example of nudge letter**

Tax administrations can send nudge letters as an initial warning to prompt taxpayers to check their returns and take action to rectify any mistakes before a more official investigation is launched.

"The [tax authority of jurisdiction] has information that show you may have received foreign income or gains and that you may have to pay [tax authority of jurisdiction] tax on your foreign income and gains. The [tax authority of jurisdiction] has received this information through the [jurisdiction]'s tax information exchange agreements with other jurisdictions.

The [tax authority of jurisdiction] wants to help make sure you are paying the right tax on your foreign income and gains.

The [tax authority of jurisdiction] has compared the information received with your tax returns. The [tax authority of jurisdiction] believes that you may not have paid the right amount of tax. There may be a reasonable explanation for this.

The [tax authority of jurisdiction] is giving you the opportunity to review your tax affairs and to tell about anything that you may need to put right.

Please help the [tax authority of jurisdiction] to make sure the information held about your tax affairs is accurate. You can do this by checking that you have told the [tax authority of jurisdiction] about all of your tax liabilities from all foreign income or gains.

[disclosure procedure to be described]"

Future non compliance

In its most sophisticated forms, data analytics can predict future taxpayer behaviour or revenue losses. This can be done by defining patterns of taxpayer behaviour, particularly with regard to tax compliance, as well as through predictive modelling to establish the risk profile of certain groups of taxpayers for future compliance activities.

- Predictive modelling uses historical information to build models that identify behaviours, attributes or patterns that correlate with known or emerging patterns of non-compliance. The models are used to create risk scores for existing taxpayers, as well as for new taxpayers and dealers. The techniques can be divided into statistical models, such as regression, or machine learning algorithms, such as decision trees and neural networks.

- Text mining can help tax authorities scan and identify phrases, patterns and entities in different sources of unstructured data (e.g. newspapers, videos, social media posts, etc.) using techniques such as natural language processing and sentiment analysis. It can improve predictive models by updating risk scores and determining the likelihood of future non-compliance through the use of more dynamic information.

Examples are provided in Box 29.

Impact assessment

Participation in CRS-AEOI requires support from decision makers and the allocation of necessary resources. Therefore, the results of the use of CRS-AEOI should be reported to decision makers as a way of demonstrating its effectiveness in enhancing the jurisdiction's domestic resources mobilisation efforts. Tracking and reporting results will also enable the government to communicate to the Parliament and the public the impact of CRS-AEOI in fighting tax evasion and other IFFs, and in increasing domestic revenue mobilisation.

The Global Forum Secretariat has created a form aimed at facilitating the work of competent authorities to collect information for assessing the CRS-AEOI impact. It adopts a format that is easy to understand and fill in.[80] This document is available upon request (gftaxcooperation@oecd.org).

8.3.3. Enhancing taxpayer compliance

The use of CRS data can also facilitate taxpayer compliance as tax administrations implement service-oriented reforms that facilitate reporting, eliminate redundant information requests and provide better targeted services based on a better understanding of taxpayers' needs and behaviours.

80. Global Forum Secretariat / OECD (2021), *Capacity-Building Tool: Exchange of Information Impact Assessment Form*.

Pre-fill of tax returns

Many tax administrations are using or considering the use of pre-filled/pre-populated returns to improve compliance, reduce taxpayer burden and simplify and streamline business processes. While these approaches currently rely heavily on the information traditionally available within a tax administration, this is changing with access to CRS data, other domestic third party data sources and the widening range and scope of administrations' pre-filling activities. To support these operations, tax administrations must have the capacity to receive information from a wide range of sources and bring it together in a consolidated manner for the taxpayer, where it can be accessed using simple intuitive interfaces. For instance, in some jurisdictions, CRS data are detailed and available in the taxpayer's account of the tax authority website.

Communication

Tax authorities' communication efforts should prompt changes in taxpayers' behaviour due to the deterrent effect of the CRS-AEOI, leading to enhanced voluntary compliance, less costs to tax authorities and much-needed tax revenue.

Aggregate statistics from jurisdictions on the data exchanged in order to better understand the extent of the exchanges is a way to demonstrate to taxpayers that there is a reasonable risk that they will be caught if they attempt to evade taxes.

Tax administrations can use CRS data to design and target voluntary compliance campaigns aimed at encouraging a specific group of potentially high-risk taxpayers to report offshore assets or income in exchange for a temporary reduction in penalties.

Policy evaluation

Although most CRS data is used to check tax compliance, it is also being used for statistics and policy evaluation. In order to better identify the extent of cross-border tax evasion, it is now possible to use CRS data that was previously unknown to tax administrations. They can now make estimates of the amount of tax losses due to undeclared assets or income and also better understand the nature and amount of financial flows between jurisdictions.

Aggregate CRS data would allow a wide range of interested stakeholders to obtain essential information on the total assets of their country's residents in financial centres. This statistical information would allow the measurement of capital flows and the identification of the most relevant financial centres chosen by a jurisdiction's residents to hold their

Box 29. **Use of data – Modelling examples**

Predictive modelling

A Predictive model can estimate the expected levels of foreign income or assets for each taxpayer, given what is known about their characteristics, behaviour and financial situation. This could be done by applying regression techniques that associate taxpayer characteristics with reported levels of income or assets. Each taxpayer would then have an actual and an expected level of foreign income or assets; cases where the actual level is significantly higher than the expected level can be investigated further.

For instance, select a certain profile from the CRS data (taxpayer, aged between X and X years old, with an income between EUR X and X, exercising a defined profession or having a defined type of asset or living in a defined region). Then pick X random taxpayers from this dataset and label them as cluster representatives. Associate each remaining item in the dataset with the nearest cluster representative for comparison to determine their actual and expected level of foreign income or assets.

Text mining

Customs and tax authorities can review social media users' profiles, photographs and posts, and use computer algorithms to detect signs of tax evasion, smuggling or undeclared income. All information that is deliberately made public by users can be collected: video, photographs, documents, etc. The public nature of the information means that it should not be necessary to register on the site or to enter a password to access it.

money and investments. For instance, tax authorities could cross-check statistical data with data reported in tax returns or with cross-border bank deposits, using datasets from the Bank for International Settlements (BIS).

Use for non-tax purposes

CRS data may also be relevant for non-tax purposes (e.g. AML/CFT purposes). The default position is that the confidentiality provisions in EOI agreements require that exchanged information must be used only in tax proceedings. However, some EOI agreements also allow for the use of treaty exchanged data for non-tax purposes provided that the conditions set out in the applicable agreement are met. For instance, Article 22(4) of the MAAC provides for the use for non-tax purposes if it is allowed under the laws of both jurisdictions and the competent authorities of the supplying jurisdiction authorises such use.

Therefore, where relevant, a receiving jurisdiction may request from its exchange partner the authorisation to use of CRS data related to a specific taxpayer for other purposes. The use for non-tax purposes will be subject to this prior authorisation and the fulfilment of the other conditions set out in the EOI agreement.

Annexes

Annex A. Glossary of concepts

This glossary provides a summary definition of key concepts used in the toolkit to facilitate the reader's understanding. It is not intended to be exhaustive. It also contains the definition of certain terms derived from the CRS-AEOI monitoring and review processes. Detailed definitions of the CRS terms are available in the CRS and its Commentary.

TERM	SUMMARY DEFINITION
Account Holder	The person listed by the Financial Institution as the holder of the account, as well as any person holding the account by means of another person such as an agent, nominee or intermediary. In the case of a Cash Value Insurance Contract or Annuity Contract, any person entitled to access the Cash Value or change the beneficiary, as well as, upon maturity any person entitled to receive payments. See CRS, Section VIII(E)(1).
Additional validation	Additional validation refers to additional checks that are not performed by the XML Validation. Additional validations include both file validations and record validations.
Automatic exchange of financial account information	This form of automatic exchange of information requires Financial Institutions to report information to their domestic tax authorities in relation to Financial Accounts held by foreign tax residents (Individuals or Entities) and, in certain cases, held by Entities controlled by foreign tax residents (defined as Controlling Persons). Tax authorities then exchange that information with the tax authorities of the jurisdictions where the Account Holder and/or Controlling Persons are tax resident.
Automatic exchange of information for tax purposes	This form of exchange of information (EOI) is the automatic exchange of a predefined set of information relevant for tax purposes between competent authorities that takes place in a systematic manner, without any prior request.
Committed jurisdiction	Global Forum member jurisdictions that have committed to start exchanging information under the CRS-AEOI standard in a particular year.
Common Transmission System	The Common Transmission System, developed under the auspices of the Forum on Tax Administration and operated within the framework the Global Forum, is the system used by all jurisdictions to transmit CRS data to exchange partners. It can also be used to transmit other EOI types.
Competent authority for exchange of information for tax purposes	An authority of a jurisdiction that is designated in an international agreement providing for the exchange of information for tax purposes as being authorised to exchange information for tax purposes with competent authorities of other jurisdictions.

TERM	SUMMARY DEFINITION
Controlling Person	The natural person who exercise control over an Entity by means of (i) beneficial ownership interest, (ii) other means or, in lack thereof, (iii) the senior managing official. In the case of a trust or similar legal arrangements (i) settlor, (ii) trustee, (iii) protectors, (iv) beneficiaries and (v) any other person exercising control over the trust. See CRS, Section VIII(D)(6).
CRS Status Message	The CRS Status Message allows the competent authority of the receiving jurisdiction to confirm acceptance or rejection of the received CRS Message to the competent authority of the sending jurisdiction, and to notify them of any errors found. It follows the CRS Status Message XML Schema.
CRS Message	This is the file transmitted by the competent authority of the sending jurisdiction to the competent authority of the receiving jurisdiction containing the CRS data. It follows the CRS XML Schema.
CRS-AEOI peers	Global Forum member jurisdictions that have committed to start exchanging information under the CRS-AEOI standard in a particular year and that have a domestic legislative framework for CRS-AEOI in place.
Diverging tax year	Situation where the tax year in a jurisdiction differs from the calendar year.
Documentary Evidence	Generally this includes certificates, identification or official documentation issued by an authorised governmental body, as well as audited financial statements, third party credit reports, bankruptcy filing, or securities regulator report. See CRS, Section VIII(D)(6).
Entity	An Entity is anything but a natural person (Individual). It includes any legal person (with its own legal personality, such as a Company) or legal arrangement (without its own legal personality, such as a trust or partnership). See CRS, Section VIII(E)(3).
Excluded Accounts	Low risk non-reportable accounts either defined in the CRS (e.g. certain retirement and pension accounts, tax favoured accounts, estate accounts, escrow accounts) or domestically defined in line with the CRS criteria. Excluded Accounts are accounts which Financial Institutions are not required to carry out due diligence on or to report on. See CRS, Section VIII(C)(17).

Annexes

TERM	SUMMARY DEFINITION
File error	A file error allows reporting that a CRS XML file has failed the file validation.
File validation	File validation verifies if the XML file can be received, read and validated. When file validation is successful, the record validation can be performed. Examples of file validation: Failed to download, decrypt, decompress, check signature, found viruses or threats, failed XML Validation, etc.
Financial Account	They are accounts maintained by Financial Institutions. They are precisely defined in the CRS. The CRS contains the following categories of Financial Accounts: (i) Depository Account, (ii) Custodial Account, (iii) Equity or Debt Interest in an Investment Entity, (iv) Cash Value Insurance Contract or (v) Annuity Contract. Financial Account does not include any account that is an Excluded Account. See CRS, Section VIII(C)(1).
Financial Institution	The Financial Institutions are precisely defined in the CRS and include (i) Depository Institution, (ii) Custodial Institution, (iii) Investment Entity and (iv) Specified Insurance Company. See CRS, Section VIII(A)(3).
Hard recommendation	Recommendation regarding serious weaknesses identified in the confidentiality and data safeguard review process.
Interested Appropriate Partners	Jurisdictions interested in receiving information and that meet the confidentially and data safeguards.
New Account	Any Financial Account opened on or after a specific date defined by the jurisdiction in its CRS legislation. Typically accounts opened on or after the date of effect of the legislation implementing the CRS. For instance, account opened on or after the 1 January of the first reportable year). See CRS, Section VIII(D)(10).
Non-Financial Entity	Any Entity other than a Financial Institution. See CRS, Section VIII(D)(7).
Non-Reporting Financial Institution	A Financial Institution exempt from complying with due diligence and reporting obligations under the CRS, either defined in the CRS (e.g. Governmental Entities, Central Banks, Qualified Credit Cards Issuers) or domestically defined in line with the CRS criteria. See CRS, Section VIII(B)(1).
Note	In the CRS-AEOI review process, notes are issued where there is lack of clarity in any aspect of the legal framework.
Participating Jurisdiction	A jurisdiction with which an agreement is in place pursuant to which it will provide CRS information and has been identified as such in a given jurisdiction list. See CRS, Section VIII(D)(5).

TERM	SUMMARY DEFINITION
Preexisting Account	Any Financial Account opened before a specific date defined by the jurisdiction in its CRS legislation. Typically accounts opened prior the date of effect of the legislation implementing the CRS. For instance, before the 1 January of the first reportable year). See CRS, Section VIII(D)(9).
Recommendation	A recommendation is issued where gaps in the domestic legislative framework implementing the CRS-AEOI standard or the effectiveness of its implementation are identified in the review process.
Record error	A record error allows reporting that a CRS XML file has failed the record validation.
Record validation	Record validation provides additional validation of the CRS data (which are not already validated by the CRS XML Schema itself). Examples of record validation: an invalid ISIN Account Number, a missing validation field, a missing DocRefID (for future corrections).
Reportable Jurisdiction	A jurisdiction with which an agreement is in place pursuant to which there is an obligation to provide CRS information and has been identified as such in a given jurisdiction list. See CRS, Section VIII(D)(4). By a slight modification of this term, a jurisdiction could implement the wider or widest approach.
Reporting Financial Institution	A Financial Institution subject to complying with due diligence and reporting obligations under the CRS (i.e. it is not a Non-Reporting Financial Institution). See CRS, section VIII(A)(1).
Soft recommendation	Recommendations issued where areas of improvement are identified in the confidentiality and data safeguard review process.
Undocumented Accounts	These are Preexisting Accounts that meet very specific requirements, indicating that there is no information available to indicate the Account Holder's residence. See CRS, Section III(B)(5), (C)(5)(c) and (C)(7), and Section IX(a)(3).
XML validation	XML validation refers to validating the CRS XML data file against the CRS XML Schema

Annex B. Substantive additional detail

The CRS Commentary contains substantive additional detail that supplements the rules contained in the CRS.[81] This detail should be incorporated in the domestic legal framework in a binding instrument.

REFERENCE	SUBSTANTIVE ADDITIONAL DETAIL
CRS Commentary, Section I, pp. 102-104	Requiring the reporting of place of birth and date of birth and the collection of Taxpayer Identification Numbers (TINs). The place of birth is not required to be reported unless the Reporting Financial Institution is otherwise required to obtain and report it under domestic law and it is available in the electronically searchable data maintained by the Reporting Financial Institution.
CRS Commentary, Section III, pp. 111-113	Where the residence address test is allowed for (see Subsection 6.3.10 of the toolkit), the provisions relating to dormant accounts, the Documentary Evidence that can be relied on and the treatment of accounts opened at a time prior to AML/KYC requirements.
CRS Commentary, Section III, pp. 115 (para. 13)	Applying the change of circumstances provisions to the residence address test (these provisions are explicitly provided for in the electronic records test, but the CRS does not apply them directly to the residence address test).
CRS Commentary, Section VI, pp. 148	Ensuring that Financial Institutions must rely only on a self-certification from either the Account Holder or the Controlling Person to determine whether a Controlling Person of a Passive NFE is a Reportable Person.
CRS Commentary, Section VIII, pp. 158-159	The definition of the residence of a Financial Institution.
CRS Commentary, Section VIII, p. 176	The approach taken when considering whether a Financial Institution maintains an account.
CRS Commentary, Section VIII, p. 192	The treatment of trusts that are Non-Financial Entities.
CRS Commentary, Section VIII, p. 200	The procedure when reporting information in relation to jointly held accounts.

81. See the OECD (2018), *Standard for Automatic Exchange of Financial Information in Tax Matters - Implementation Handbook*, op.cit., pp. 19-22.

REFERENCE	SUBSTANTIVE ADDITIONAL DETAIL
CRS Commentary, Section VIII, p. 116 (para. 17)	Definition of the term "change in circumstances".
CRS Commentary, Section IX, p. 208	Imposing sanctions for providing false self-certifications.
CRS Commentary, Section V, p. 148	Explicitly requiring that the status of the New Entity Account is to be re-determined in cases of a change in circumstances that causes the Financial Institution to have reason to know that the self-certification or other documentation associated with the account is incorrect or unreliable.
CRS Commentary, Section IX, p. 209	Ensuring that the records of the steps undertaken and any evidence relied upon for the purposes of the due diligence provisions are available for a period of at least 5 years after the end of the relevant reporting date.
CRS, Section VIII(D)(6) **CRS Commentary, Section VIII, pp. 198-199**	The definition of Controlling Persons is an important additional detail provided in the Commentary that supplements the CRS. It must be construed in such a manner to correspond to the definition of the term "beneficial owner" as described in the Financial Action Task Force ("FATF") Recommendation 10 and the accompanying Interpretative Note as adopted in February 2012. The Commentary further clarifies that the AML/KYC process adopted to determine the Controlling Persons of an Account Holder of a New Entity Account must be in line with both FATF 2012 Recommendations 10 and 25 and their Interpretative Notes. Accordingly, the Controlling Persons are the natural persons who are in control of the Account Holders of the New Entity Accounts (including through a chain of ownership or control).

Annex C. Model rules based on the "reference" method

The Global Forum Secretariat has developed models of legislation based on the "copy out" and "reference" methods.

Annex C provide a model rules based on the "reference method" which would allow a jurisdiction to fully implement the CRS and its Commentary through a single legislative instrument.

Model legislation following the "copy out" approach is also available to competent authorities upon request (gftaxcooperation@oecd.org).

Even where the model rules are adopted with minimal change, jurisdictions may still wish to create guidance to aide understanding by their Financial Institutions of their new obligations.

The Global Forum Secretariat remains available to assist implementing jurisdictions in the drafting of their CRS domestic legislation to ensure that it meets the Standard.

Provisions	Comments
1. Short title and commencement	This Section of the model rules is an example that should be adapted based on the legal tradition of the jurisdiction.
This Act may be cited as the Automatic Exchange of Financial Account Information Act, [year] and comes into force by Order on a date fixed by the [Relevant authority] of [Jurisdiction].	
2. Definitions	This Section of the model rules contains the definition of the relevant terms used in this Act. The other terms used in the Common Reporting Standard (CRS) are defined by reference.
1) In this Act, "**Agreement**" means a) the Convention on Mutual Administrative Assistance in Tax Matters, which provides for the exchange of information on an automatic basis as described in the Standard, signed by [Jurisdiction] on [date] [set out in Schedule 1], as amended from time to time, and b) the Multilateral Competent Authority Agreement on Automatic Exchange of Financial Account Information signed by [Jurisdiction] on [date] [set out in Schedule 2].	In this model, it is assumed that the international legal framework used is the Convention on Mutual Administrative Assistance in Tax Matters (MAAC) and the Multilateral Competent Authority Agreement on Automatic Exchange of Financial Account Information (CRS MCAA). Depending on the legal tradition of the implementing jurisdiction, the MAAC and/or the CRS MCAA can be added as a Schedule to the Act. In particular, this can be necessary if the Act will also give force of law to the MAAC and/or CRS MCAA. See Part 5 of the toolkit.

Provisions	Comments
"[**Commissioner**]" means [the Commissioner] as defined in the [Tax Administration Act].	The jurisdiction would refer to the appropriate administrator (Commissioner, Comptroller, Director or other), which may be an officeholder or an administrative authority.
"**Designated officer**" means, which respect to any function, an officer of the [Tax authority] designated to carry out that function. "**Information return**" means a report, setting out certain information as specified in the Standard and any further information specified by regulations made under this Act, which a Reporting Financial Institution is required to file with the [Commissioner]. "**Minister**" means the [Minister responsible for Finance].	These definitions should be adapted by the implementing jurisdictions taking into account their own context. In these model rules, the tax authority is the administering authority of the CRS legislation. This function is shared in some jurisdictions with other authorities, in particular with respect to the enforcement of the CRS legislation (e.g. tax authority or financial sector regulators) (see Subsection 7.1 of the toolkit). Depending on the domestic arrangement, this provision should be adapted. However, the definition of the "Information return" is linked to key other elements of the "reference" approach used in this Act (Standard, Reporting Financial Institution). Therefore, any change should be considered carefully.
"**Reportable Account**" means an account held by one or more Reportable Persons or by a Passive NFE with one or more Controlling Persons that is a Reportable Person, provided it has been identified as such pursuant to the due diligence procedures described in Sections II through VII of the Standard, or would have been identified as such if those procedures had been correctly applied.	This term is precisely defined in the CRS. The proposed definition makes a clear reference to the Standard. Any amendment to this definition should be considered carefully. See Section 2.3 of the toolkit.
"**Participating Jurisdiction**" means a jurisdiction identified as such on a list published by [the Ministry/Tax authority].	This term is defined in the CRS as a jurisdiction with which an agreement is in place pursuant to which it will provide CRS information and has been identified as such in a given jurisdiction list. To simplify, the model rules directly refer to the published list. It is recommended to have the list in legal instrument that can be easily modified (e.g. secondary legislation, binding guidance, etc.) to take into account that new jurisdictions are implementing the Standard and will be added in the list in the future.

Provisions	Comments
"**Reportable Jurisdiction**" means **a)** for the purposes of applying the due diligence procedures described in Section II to VII of the Standard, a jurisdiction other than [Jurisdiction], and **b)** for the purposes of reporting the information required by Section I of the Standard, a jurisdiction identified as such on a list published by [the Ministry/Tax authority].	This term is defined in the CRS as a jurisdiction with which an agreement is in place pursuant to which there is an obligation to provide CRS information and has been identified as such in a given jurisdiction list. The definition provided in this model adopts the "wider approach" (see Subsection 6.3.20 of the toolkit): Financial Institutions are required to perform the CRS due diligence on all their Financial Accounts but are only required to report information on the Reportable Persons that are resident in one of the jurisdictions included in the list. The jurisdiction may alternatively revise the definition to limit it to only those jurisdictions required for exchange of account information: "***Reportable Jurisdiction***" *means a jurisdiction identified as such on a list published by [the Ministry/Tax authority].*" If the jurisdiction opts to adopt the "widest approach" then a) and b) can be merged: "***Reportable Jurisdiction***" *means for the purposes of applying the due diligence and reporting procedures described in Section I to VII of the Standard, a jurisdiction other than [Jurisdiction].*"
"**Reporting Financial Institution**" means any [Jurisdiction] Financial Institution that is not a Non-Reporting Financial Institution. The term "[Jurisdiction] Financial Institution" means: (i) any Financial Institution that is resident in [Jurisdiction], but excludes any branch of that Financial Institution that is located outside of [Jurisdiction]; and (ii) any branch of a Financial Institution that is not resident in [Jurisdiction], if that branch is located in [Jurisdiction].	This definition is aligned with the CRS definition and should not be modified.
"**Standard**" means the Common Reporting Standard, including the Commentary thereon, approved by the Council of the Organisation for Economic Co-operation and Development on 15 July 2014, which contains reporting and due diligence procedures for the exchange of information on an automatic basis, as amended from time to time.	This definition is central to the "reference" method. It refers to the CRS and its Commentary. This definition should not be modified.
(2) Any word or expression which has a meaning given to it by the Standard shall, where it is used in this Act or regulations made under this Act and unless the contrary intention appears, have the same meaning in this Act and those regulations as it has in the Standard.	This provision ensures that the CRS definitions are transposed into domestic CRS legislation.

Provisions	Comments
3. Agreement – force of law The Agreement is approved and has the force of law in [Jurisdiction].	This Section aims at giving force of law to the MCAA and/or the CRS MCAA. This provision may not be necessary depending on the status of these agreements in the jurisdiction and its legal tradition. See also the comments on Section 2 of these model rules.
4. Inconsistent laws In the event of any inconsistency between the provisions of this Act or the Agreement and the provisions of any other law, the provisions of this Act and the Agreement prevail to the extent of the inconsistency.	This Section is intended to override other legal provisions in force. This can be used alongside Section 7(1) below as a specific override clause in respect of any pre-existing secrecy or confidentiality provisions that are in conflict with this Act. See Subsection 6.2.7 of this toolkit.
5. Information returns by Reporting Financial Institutions	This Section imposes due diligence and reporting obligations on Reporting Financial Institutions with reference to the relevant Sections of the Standard (CRS and Commentary).
(1) A Reporting Financial Institution shall file an information return with the [Commissioner] in respect of all Reportable Accounts it maintains in a calendar year, with the information described in Section I of the Standard, on or before [31 May] of the year following the calendar year to which the information relates.	This Subsection creates the reporting obligation. The information to be reported is the one provided in the Standard. The date chosen for the reporting is an example. The 31 May gives Reporting Financial Institution five months to collect and submit the information, and it gives the jurisdiction four months to prepare and transmit the information to exchange partners. Other dates may be considered suitable. See Subsection 6.2.2 of the toolkit.
(2) Whether a Reporting Financial Institution maintains a Reportable Account must be determined by the Reporting Financial Institution by applying the due diligence procedures described in Sections II through VII of the Standard.	This Subsection of the model rules creates the due diligence obligation, which are described in details in the relevant Sections of the Standard.
(3) A Reporting Financial Institution shall file an information return in the manner and form specified by the [Commissioner].	This optional provision can be used if the jurisdiction requires or wishes that the manner of reporting be included in a binding instrument. See Subsection 6.2.2 of the toolkit.
(4) A Reporting Financial Institution that does not maintain a Reportable Account in a calendar year shall file a nil return.	The nil reporting is a useful requirement to ensure compliance of Financial Institutions with their CRS obligations. It is recommended to include this optional provision. See Subsection 6.3.6 and Section 7.1 of the toolkit.

Provisions	Comments
6. Functions and powers of the [Commissioner]	This Section provides for the functions and the powers of the relevant authority for the administration and enforcement of the CRS legislation. The approach taken in these model rules is that the tax authority will be in charge of all aspects of the administration and enforcement of the CRS legislation. Where other authorities (e.g. regulators) are involved in the enforcement of the CRS legislation, this Section may need to be adapted accordingly. Some or all of these powers may already exist under other tax law (or other legislation), in which case it may be unnecessary for all elements to be included in CRS implementation law. The powers mentioned in Subsection (4) should be available to the authority in charge of the enforcement of the CRS legislation. In any case, the implementing jurisdiction should ensure that the competent authority has the access and information gathering powers necessary to ensure effective implementation. See Subsection 6.2.4 and Section 7.1 of the toolkit.
(1) The [Commissioner] shall generally administer and enforce compliance with the provisions of the Agreement, this Act and any regulations made under this Act.	
(2) The [Commissioner] may exercise all powers vested in him under the [Tax Administration Act] to administer and enforce compliance with this Act and any regulations made under this Act.	
(3) The [Commissioner] may delegate, in writing, to any designated officer any power or duty conferred on the [Commissioner] by this Act.	
(4) The [Commissioner] or any designated officer may request information from and, at all reasonable times, enter any premises or place of business of a Reporting Financial Institution for the purposes of: **a)** determining whether information (i) included in an information return made under the regulations by the Reporting Financial Institution is correct and complete, or (ii) not included in an information return was correctly not included; or **b)** examining the procedures put in place by the Reporting Financial Institution for the purposes of ensuring compliance with that institution's obligations under this Act and the regulations.	

Provisions	Comments
7. Confidentiality	An implementing jurisdiction may already have similar provisions under other tax law ensuring confidentiality of the data and legal protection to Financial Institutions and their personnel when they provide required information to the tax authority. Where similar provisions already exist, it may be unnecessary to include in the CRS implementation law.
(1) Any person who divulges any confidential information or provides information to the [Tax authority] in conformity with Sections 5 and 6 of this Act shall, by reason only of such disclosure or the provision of such information, be deemed not to commit any offence under any other law in force in [Jurisdiction] and not to be a breach of any confidential relationship between that person and any other person.	This subparagraph is intended to override any pre-existing secrecy or confidentiality provisions in force, and to relieve any persons obligated to report the CRS information (Financial Institutions and their personnel) of any sanctions that would otherwise be imposed for this disclosure of information. This can be used alongside Section 4 above. See Subsection 6.2.7 of this toolkit.
2) Any person being employed or formerly employed in the administration or enforcement of this Act or the regulations made under this Act shall treat information received from a Financial Institution under this Act or those regulations as confidential and shall only disclose such information as may be necessary for the purpose of the administration or enforcement of the Agreement, this Act or under those regulations. (3) A person who discloses or divulges any information or produces any document relating to the information received from a Financial Institution under this Act or the regulations made under this Act in contravention of Subsection (2) commits an offence and is liable, on summary conviction, to a fine of [amount] [and / or] [to a term of imprisonment not exceeding] [one year].	Subsections (2) and (3) are intended to ensure that persons such as officials or employees of the tax administration handle the information received from a Reporting Financial Institution in the course of their duties in a confidential manner.

Provisions	Comments
8. Record keeping (1) A Reporting Financial Institution must keep records of the steps undertaken and any evidence relied upon for the purpose of complying with this Act or regulations made under this Act. (2) The records required to be kept under this Section must be retained for a period not less than five years after [31 May] of the year following the calendar year to which the records relate.	This provision sets out the record-keeping obligations. The date chosen as the due date for filing information returns is 31 May in the model rules. The implementing jurisdiction can choose a different date taking into account (i) the time needed for the Financial Institutions to prepare and submit their files to the tax authority and the time needed for the competent authority to prepare and transmit the files to its exchange partners. A retention period of less than five years after the due date for filing information returns (31 May in the model rules) would not meet requirements of the standard. See Subsection 6.2.3 of the toolkit.
9. Penalties (1) Any Reporting Financial Institution that fails to file an information return as and when required under this Act or under regulations made under this Act is liable to a penalty of [amount] for each such failure, and the product obtained when [amount] is multiplied by the number of days, not exceeding [number], during which the failure continues. (2) Any person who makes a false statement or omission in respect of any information required to be included on an information return, under this Act or under regulations made under this Act, is liable to a penalty of [amount] for each such failure. (3) Any person who makes a false statement or omission in respect of information in a self-certification made for the purposes of the due diligence procedures described in the Standard is liable to a penalty of [amount]. (4) Any person who does not comply with the requirement of the [Commissioner] or a designated officer in the exercise or performance of the [Commissioner's] or officer's powers or duties under this Act or under regulations made under this Act is liable to a penalty of [amount] for each such failure. (5) Any person who fails to comply with a duty or obligation imposed by this Act or under regulations made under this Act that is not otherwise described in this Section is liable to a penalty of [amount] for each such failure.	This Section provides for sanctions to address non-compliance. For details on all aspects of non-compliance which penalties should address and other considerations see Subsection 6.2.5 of the toolkit. Subsection (4) of the model rules may already be covered under other tax law, in which case it will be unnecessary to include in CRS implementation law.

Provisions	Comments
10. Liabilities to penalties	Sections 10 to 14 provide model provisions to ensure effective sanction of non-compliance. These Sections of the model rules, or some parts of these, may already be covered under other tax law, in which case it may be unnecessary to include the relevant provisions in CRS implementation law. An implementing jurisdiction should assess whether these provisions are not already provided in the domestic legal framework or adapt these provisions to its legal tradition.
(1) Liability to a penalty under Section 9 does not arise if the person satisfies the [Commissioner] that there is a reasonable excuse for the failure. (2) For the purposes of this Act neither of the following is a reasonable excuse **a)** that there is an insufficiency of funds to do something, or **b)** that a person relies upon another person to do something. (3) If a person had a reasonable excuse for a failure but the excuse has ceased, the person is to be treated as having continued to have the excuse if the failure is remedied without unreasonable delay after the excuse ceased.	
11. Assessment of penalties	
(1) If a person becomes liable to a penalty under Section 9, the [Commissioner] shall **a)** assess the penalty, and **b)** notify the person of the assessment. (2) An assessment of a penalty under Section 9 shall be made within the period of 12 months beginning with the date on which the failure or inaccuracy first came to the attention of the [Commissioner].	
12. Right to appeal against penalties	
A person may appeal against a penalty assessment **a)** on the grounds that liability to a penalty under Section 9 does not arise, or **b)** on the amount of such a penalty.	

Provisions	Comments
13. Procedure on appeal against penalty	
(1) Notice of an appeal under Section 11 shall **a)** be provided to the [Commissioner], in writing, before the end of the period 30 days beginning with the date on which notification under Section 11 was provided, and **b)** set out the grounds of appeal. (2) On an appeal under Section 12(a) that is notified to the [Commissioner], the [Commissioner] may confirm or cancel the assessment. (3) On appeal under Section 12(b) that is notified to the [Commissioner], the [Commissioner] may confirm the assessment or substitute another assessment that the [Commissioner] had power to make. (4) Subject to this section and Section 14, the provisions of the [Tax Administration Act] relating to appeals shall apply in relation to appeals under Section 12 as they apply in relation to an appeal against a tax assessment.	
14. Enforcement of penalties	
(1) A penalty under this Act shall be paid to [Tax authority] within 30 days after **a)** the date on which notification under Section 11 is provided in respect of the penalty, or **b)** the date on which an appeal against a penalty assessment pursuant to Section 9 is finally determined or withdrawn. (2) If any amount in respect of a penalty is not paid by the due date described in subsection (1), interest on the amount owing shall be charged computed for the period during which that amount is outstanding. (3) The rate of interest charged under subsection (3) shall be [percentage] per annum.	
15. Anti-avoidance	This applies the null and void approach to prevent persons from circumventing the reporting and due diligence procedures. See Subsection 6.2.6 of the toolkit.
If a person enters into any arrangements or engages in a practice, the main purpose or one of the main purposes of which can reasonably be considered to be to avoid an obligation imposed under this Act or regulations made under this Act, this Act and regulations made under this Act shall have effect as if the person had not entered into the arrangement or engaged in the practice.	

Provisions	Comments
16. Regulations The Minister may make any regulations that are necessary for carrying out the Agreement, this Act, or for giving effect to any of the provisions of the Agreement or this Act.	This provisions allow the Minister to make any regulations necessary for the implementation of the CRS. Under these model rules most of the implementing provisions are introduced through the reference approach. This provision may be necessary where (i) some aspects of the CRS implementation cannot be introduced through guidance (e.g. technical requirement for the reporting) or (ii) where the provisions of Section 17 of the model rules should be introduced in secondary legislation.
17. Modifications and options applied to the Standard	This Section of the model rules allow to modify certain provisions of the Standard to introduce optional provisions (Subsections (1)-(5)) or introduce the necessary date for the CRS due diligence and reporting obligations. Any or all of these provisions could be relegated to Regulations.
For the purposes of this Act and regulations made under this Act [(1) Entities described in Schedule 3 are Non-Reporting Financial Institutions under subparagraph B.1(c) of Section VIII of the Standard].	This Subsection allows for the introduction of a jurisdiction-specific list of Non-Reporting Financial Institutions. See Subsection 6.3.1 of the toolkit.
[(2) The accounts described in Schedule 4 are Excluded Accounts under subparagraph C(17)(g) of Section VIII of the Standard].	This Subsection allows for the introduction of a jurisdiction-specific list of Excluded Accounts. See Subsection 6.3.2 of the toolkit.
[(3) To the extent that the Standard and the Agreement give [Jurisdiction] the ability to provide for an Entity to make an election or choice in determining obligations under the Standard, the Entity may make the election or choice.]	This provision allows the Entities to benefit from all the provision of the Standard providing for an election or a choice. The jurisdiction may modify it by listing only some of the elections, or exclude some of the elections. See Subsections 6.3.4, 6.3.7-6.3.13, and 6.3.19 of the toolkit.
[(4) The Standard has effect with the following modifications mentioned in the Commentary: a) the inclusion mentioned in paragraph 13 of the Commentary on Section VII concerning Special Due Diligence Requirements; and b) the two replacements mentioned in paragraph 82 of the Commentary on Section VIII.]	Subsection (a) provides for the alternative documentation procedure for certain Group Insurance Contracts or Annuity Contracts. See Subsection 6.3.12 of the toolkit. Subsection (b) provides for the expanded Definition of a Preexisting Account and expanded definition of a Related Entity. See Subsections 6.3.16 and 6.3.17 of the toolkit.

Provisions	Comments
[(5) Paragraph F of Section I of the Standard is to be disregarded.]	Jurisdictions carrying out exchanges under the MCAA or a version of the Model CAA must disregard Paragraph F of Section I by including this subsection or similar. Paragraph F concerns the phasing of the requirement to report gross proceeds. See Subsection 6.3.5 of the toolkit.
(6) The relevant dates to be applied in the Standard are: **a)** for subparagraphs C.9 (Preexisting Account), C.14 (Lower Value Account) and C.15 (High Value Account) of Section VIII – 31 December [year-1] **b)** for subparagraph C.10 (New Account) of Section VIII – 1 January [year 0] **c)** for subparagraph C.6 of Section III – 31 December [year-1] **d)** for paragraph D of Section III (completion date for review of Preexisting Individual Accounts) – 31 December [year 0]; **e)** for each occurrence in paragraphs A and B of Section V – 31 December [year-1] **f)** for the first occurrence in subparagraph E.1 and the occurrence in subparagraph E.2 of Section V – 31 December [year-1] **g)** for the second occurrence in subparagraph E.1 of Section V – 31 December [year+1] **h)** for subparagraphs B.8 (Qualified Credit Card Issuer) and C.17(f) (an account with an excess payment) of Section VIII – 1 January [year 0] **i)** for subparagraph B.9 (Exempt Collective Investment Vehicle) of Section VIII, the two dates are 1 January [year 0] and 31 December [year+2] respectively.	This Subsection introduces the relevant date. In this subsection "year 0" refers to the year of the first reportable period starting on 1 January. The date is a decision for the jurisdiction, however for High Value Accounts it is expected to be the date a year after the date selected to define Preexisting Accounts and up to a further year later in the case of Lower Value Accounts. A jurisdiction choosing to have different dates for High Value and Lower Value Accounts could word Subsection (6)(d) as follows: "for paragraph D of Section III (completion date for review of Preexisting Individual Accounts) the date is 31 December [year 0] in the case of High Value Accounts and 31 December [year+1] in the case of Lower Value Accounts". Regarding Subsection (6)(d), the date is expected to be the same date as that selected to define New Accounts. Regarding Subsection (6)(i), the jurisdiction may alternatively choose to restrict the definition of Exempt Collective Investment Vehicle only to the first paragraph of the definition in the Standard. In such a case, it will be unnecessary to provide dates here. The jurisdiction would need to add a subsection here (or in the regulations) similar to the following: "*The definition of "Exempt Collective Investment Vehicle" in subparagraph B.9 of Section VIII of the Standard is limited to the first sentence only*". See Subsection 6.3.18 of the toolkit. For details on what jurisdictions should consider when determining the relevant dates for due diligence, see Subsection 6.2.1 of the toolkit.

Provisions	Comments
(7) For the purposes of the Standard, the threshold for "controlling ownership interest" in a legal person is [X%]/[the threshold applied in the AML law].	This Subsection clarifies the threshold for determining controlling ownership interest in a legal person for the purposes of paragraph 133 of the Commentary to Section VIII. This threshold cannot be higher than the threshold to determine beneficial owner for AML/CFT purposes, although it may be lower. See Subsection 6.1.3 and Box 8 of this toolkit. Jurisdictions may choose to insert directly the percentage into Subsection (7) or to refer to the threshold set out in their AML/CFT law, in which case they should reference that particular AML/CFT legislation.

Annex D. Documentation

Reference documents on the Standard for Automatic Exchange of Financial Information in Tax Matters

- Global Forum Secretariat / OECD (2021), *Peer Review of the Automatic Exchange of Financial Account Information 2021*, available at https://doi.org/10.1787/90bac5f5-en.

- Global Forum Secretariat / OECD (2021), *Unleashing the potential of automatic exchange of information for developing countries – 2021 Strategy*, available at www.oecd.org/tax/transparency/documents/aeoi-strategy-developing-countries.pdf.

- Global Forum Secretariat / OECD (2020), *Peer Review of the Automatic Exchange of Financial Account Information 2020*, available at https://doi.org/10.1787/175eeff4-en.

- OECD (2020), *Automatic Exchange of Information: Guide on Promoting and Assessing Compliance by Financial Institutions*, Paris, available at www.oecd.org/tax/forum-on-tax-administration/publications-and-products/automatic-exchange-of-information-guide-on-promoting-and-assessing-compliance-by-financial-institutions.htm.

- OECD (2019), *Common Reporting Standard Status Message XML Schema: User Guide for Tax Administrations*, Version 2.0 – June 2019, OECD, Paris, available at www.oecd.org/tax/exchange-of-tax-information/common-reporting-standard-status-message-xml-schema-user-guide-for-tax-administrations-june-2019.pdf.

- OECD (2019), *Common Reporting Standard XML Schema: User Guide for Tax Administrations*, Version 3.0 – June 2019, OECD, Paris, available at www.oecd.org/tax/exchange-of-tax-information/common-reporting-standard-xml-schema-user-guide-for-tax-administrationsjune-2019.pdf.

- OECD (2019), *CRS-related Frequently Asked Questions*, available at www.oecd.org/tax/automatic-exchange/common-reporting-standard/CRS-related-FAQs.pdf.

- OECD (2019), *CRS Status Message XML Schema*, Version 2.0 available at www.oecd.org/tax/automatic-exchange/publications/common-reporting-standard-status-message-xml-schema-user-guide-for-tax-administrations.htm.

- OECD (2019), *CRS XML Schema*, Version 2.0, available at www.oecd.org/tax/automatic-exchange/common-reporting-standard/schema-and-user-guide.

- OECD (2019), *International Exchange Framework for Mandatory Disclosure Rules on CRS Avoidance Arrangements and Opaque Offshore Structures*, OECD, Paris, available at www.oecd.org/tax/exchange-of-tax-information/international-exchange-framework-for-mandatory-disclosure-rules-on-crs-avoidance-arrangements-and-opaque-offshore-structure.pdf.

- OECD (2018), *Model Mandatory Disclosure Rules for CRS Avoidance Arrangements and Opaque Offshore Structures*, OECD, Paris, available at www.oecd.org/tax/exchange-of-tax-information/model-mandatory-disclosure-rules-for-crs-avoidance-arrangements-and-opaque-offshore-structures.pdf.

- Global Forum / OECD (2018), *The framework for the full AEOI reviews: the Terms of Reference*, available at www.oecd.org/tax/transparency/documents/AEOI-terms-of-reference.pdf.

- OECD (2018), *Standard for Automatic Exchange of Financial Information in Tax Matters - Implementation Handbook* – Second Edition, OECD, Paris, available at www.oecd.org/tax/exchange-of-tax-information/implementation-handbook-standard-for-automatic-exchange-of-financial-account-information-in-tax-matters.htm.

- OECD (2017), *Standard for Automatic Exchange of Financial Account Information in Tax Matters*, Second Edition, OECD Publishing, Paris, available at http://dx.doi.org/10.1787/9789264267992-en.

Reference documents on confidentiality and data safeguards

- Global Forum Secretariat / OECD (2020), *Confidentiality and Information Security Management Toolkit*, available at www.oecd.org/tax/transparency/documents/confidentiality-ism-toolkit_en.pdf.

- Global Forum / OECD (2018), *Terms of Reference for Confidentiality and Data Safeguards Assessments*, available at www.oecd.org/tax/transparency/documents/confidentiality-data-safeguards-assessments-tor.pdf.

Reference documents on other forms of automatic or mandatory spontaneous exchange

- OECD (2019), *Mandatory Disclosure Rules XML Schema* Version 1.0 available at www.oecd.org/ctp/exchange-of-tax-information/international-exchange-framework-for-mandatory-disclosure-rules-on-crs-avoidance-arrangements-and-opaque-offshore-structures.htm.

- OECD (2019), *Substantial Activities in No or Only Nominal Tax Jurisdictions: Guidance for the Spontaneous Exchange of Information*, OECD, Paris, available at www.oecd.org/tax/beps/substantial-activities-in-no-or-only-nominal-tax-jurisdictions-guidance-for-the-spontaneous-exchange-of-information.htm.

- OECD (2019), *Country-by-Country Reporting XML Schema* Version 2.0 available at www.oecd.org/tax/country-by-country-reporting-xml-schema-user-guide-for-tax-administrations.htm.

Annexes

- OECD (2019), *Country-by-Country Reporting XML Schema: User Guide for Tax Administrations*, Version 2.0 – June 2019, OECD, Paris, available at www.oecd.org/tax/beps/country-by-country-reporting-xml-schema-user-guide-for-tax-administrations-june-2019.pdf.

- OECD (2015), *Mandatory Disclosure Rules*, Action 12 - 2015 Final Report, OECD/G20 Base Erosion and Profit Shifting Project, OECD Publishing, Paris, available at http://dx.doi.org/10.1787/9789264241442-en.

- OECD (2015), *Countering Harmful Tax Practices More Effectively, Taking into Account Transparency and Substance*, Action 5 - 2015 Final Report, OECD/G20 Base Erosion and Profit Shifting Project, OECD Publishing, Paris, available at http://dx.doi.org/10.1787/9789264241190-en.

- OECD (2015), *Transfer Pricing Documentation and Country-by-Country Reporting*, Action 13 - 2015 Final Report, OECD/G20 Base Erosion and Profit Shifting Project, OECD Publishing, Paris, available at http://dx.doi.org/10.1787/9789264241480-en.

Other relevant information

- Automatic Exchange Portal, accessible at www.oecd.org/tax/automatic-exchange.

- Global Forum on Transparency and Exchange of Information for Tax Purposes website, accessible at www.oecd.org/tax/transparency.

- Global Forum Secretariat / OECD (2021), *Tax Transparency in Africa, Africa Initiative Progress Report 2020*, available at www.oecd.org/tax/transparency/documents/Tax-Transparency-in-Africa-2021.pdf.

- Global Forum Secretariat / OECD (2020), *Capacity Building: A new strategy for the widest impact*, available at www.oecd.org/tax/transparency/what-we-do/technical-assistance/Capacity-Building-Strategy.pdf.

- Global Forum Secretariat / OECD (2020), *Tax Transparency in Africa, Africa Initiative Progress Report 2019*, available at www.oecd.org/tax/transparency/documents/Tax-Transparency-in-Africa-2020.pdf.

- Global Forum Secretariat / OECD (2019), *Tax Transparency in Africa, Africa Initiative Progress Report 2018*, available at www.oecd.org/tax/transparency/documents/africa-initiative-report-2018.pdf.

- OECD (2017), *Model Tax Convention on Income and on Capital: Condensed Version 2017*, OECD Publishing, available at http://dx.doi.org/10.1787/mtc_cond-2017-en.

- Global Forum / OECD (2017), *The Global Forum's Plan of Action for Developing Countries Participation in AEOI*, available at www.oecd.org/tax/transparency/documents/plan-of-action-AEOI-and-developing-countries.pdf.

- OECD (2015), *Update on Voluntary Disclosure Programmes – A Pathway to Tax Compliance*, available at www.oecd.org/ctp/exchange-of-tax-information/Voluntary-Disclosure-Programmes-2015.pdf.

- OECD (2014), *Multilateral Competent Authority Agreement on Automatic Exchange of Financial Account Information*, available at www.oecd.org/tax/automatic-exchange/international-framework-for-the-crs/multilateral-competent-authority-agreement.pdf.

- OECD and Council of Europe (2011), *The Multilateral Convention on Mutual Administrative Assistance in Tax Matters: Amended by the 2010 Protocol*, OECD Publishing, available at http://dx.doi.org/10.1787/9789264115606-en.

- O'Reilly P., Ramirez K.P. and Stemmer M.A. (2019), *Exchange of Information and Bank Deposits in International Financial Centres*, OECD Taxation Working Papers, No. 46, OECD Publishing, Paris, available at https://doi.org/10.1787/025bfebe-en.

Annex E. Donors of the Global Forum capacity-building programme

Since 2011, the Global Forum has delivered a capacity-building programme to support the implementation of the two global standards on transparency and exchange of information by its developing members and effective use of the information exchanged. Our activities are empowering jurisdictions in their fight against tax evasion and other illicit financial flows, and ultimately helping them enhance their domestic resource mobilisation.

Our capacity-building programme has developed and expanded over the years. Today, more than half of the Global Forum members are developing countries. The programme aims to ensure that developing jurisdictions are not left behind, and fully benefit from the remarkable progress achieved in transparency and administrative co-operation in the past decade. To that end, the Global Forum Secretariat works closely with regional and global partner organisations.

Through awareness raising at political level, training of thousands of officials, the development of tools (e.g. toolkits, e-learning) and high-standard technical assistance, the dynamic of change is progressing and more developing jurisdictions are reaping the benefits of a more transparent tax world.

The Toolkit for the Implementation of the Standard for Automatic Exchange of Financial Account Information will support developing countries in their implementation journey. The Global Forum Secretariat stands ready to assist them at any stage of this journey.

The delivery of the Global Forum's capacity-building programme is only made possible thanks to the financial support and the trust of our donor partners.

Financial contributions provided by:

Australia

European Union

France

Germany

Japan

Norway

Senegal

Switzerland

United Kingdom

For more information:


www.oecd.org/tax/transparency


gftaxcooperation@oecd.org


@OECDtax | #TaxTransparency