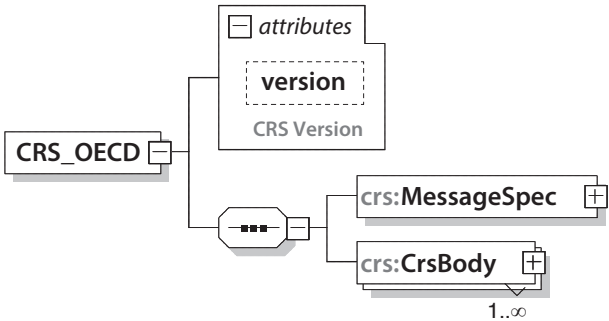## *Appendix A*

CRS XML Schema v. 1.0 Diagrams
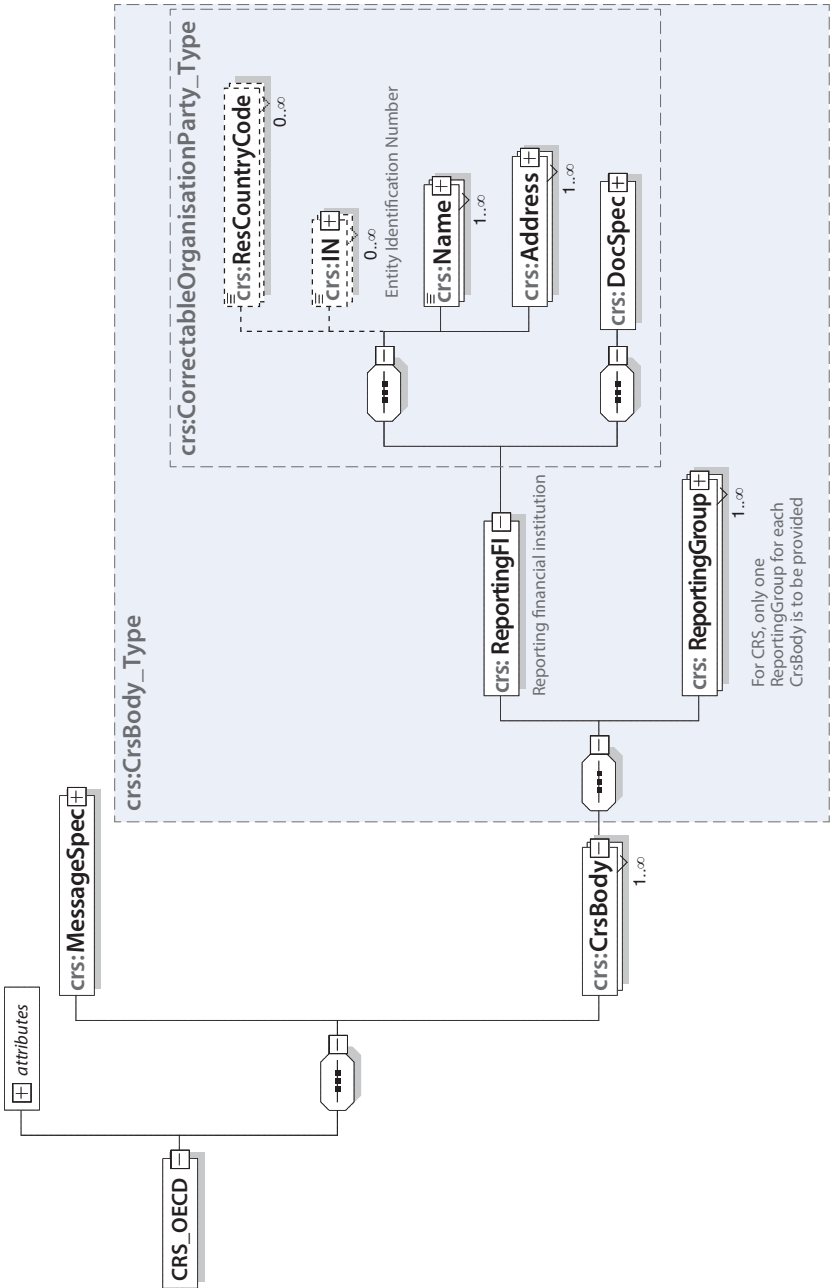
Message Header (Section I)

Information:
- Use MessageSpe. CorrMessageRefID to cancel a complete message
- MessageTypeIndic shows message type; new data / corrected data / "no data to report"

crs:MessageSpec_Type

crs:SendingCompanyIN

crs:TransmittingCountry

crs:ReceivingCountry

crs:MessageType

crs:Warning
Free text expressing the restrictions for use of the information this message contains and the legal framework under which it is given.

crs:Contact
All necessary contact information about persons responsible for and involved in the processing of the data transmitted in this message, both legally and technically. Free text as this is not intended for automatic processing.

crs:MessageRefId
Sender's unique identifier for this message

crs:MessageTypeIndic

crs:CorrMessageRefId
0..∞
Sender's unique identifier that has to be corrected. Must point to 1 or more previous messages.

crs:ReportingPeriod
The reporting year for which information is transmitted in documents of the current message.

crs:Timestamp

CRS_OECD

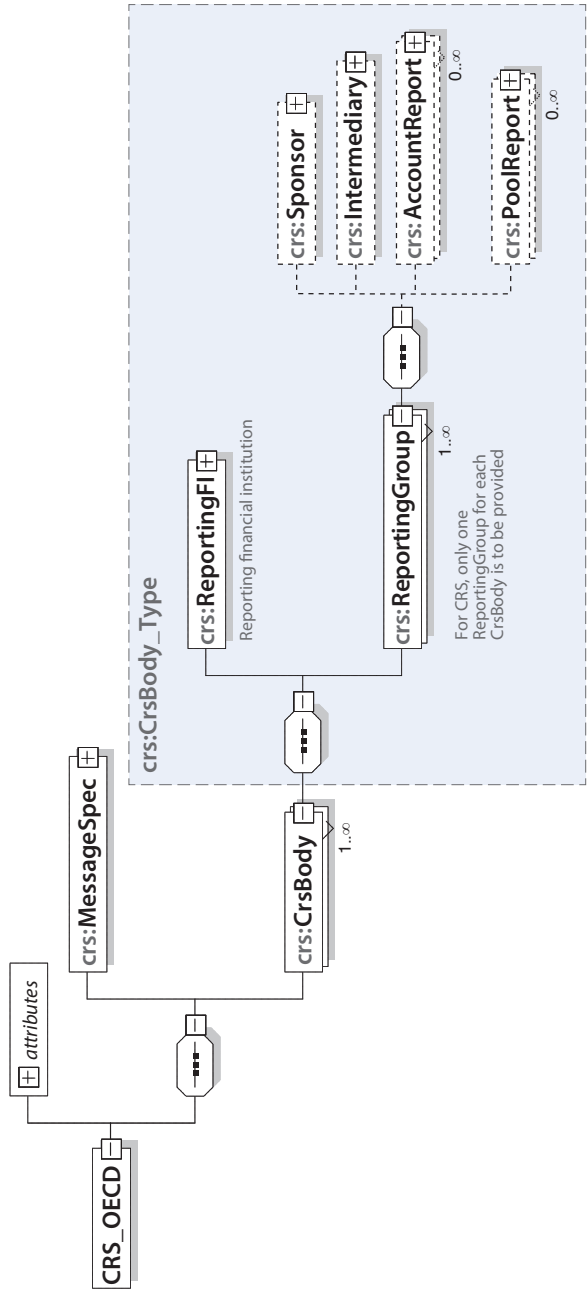attributes

crs:MessageSpec
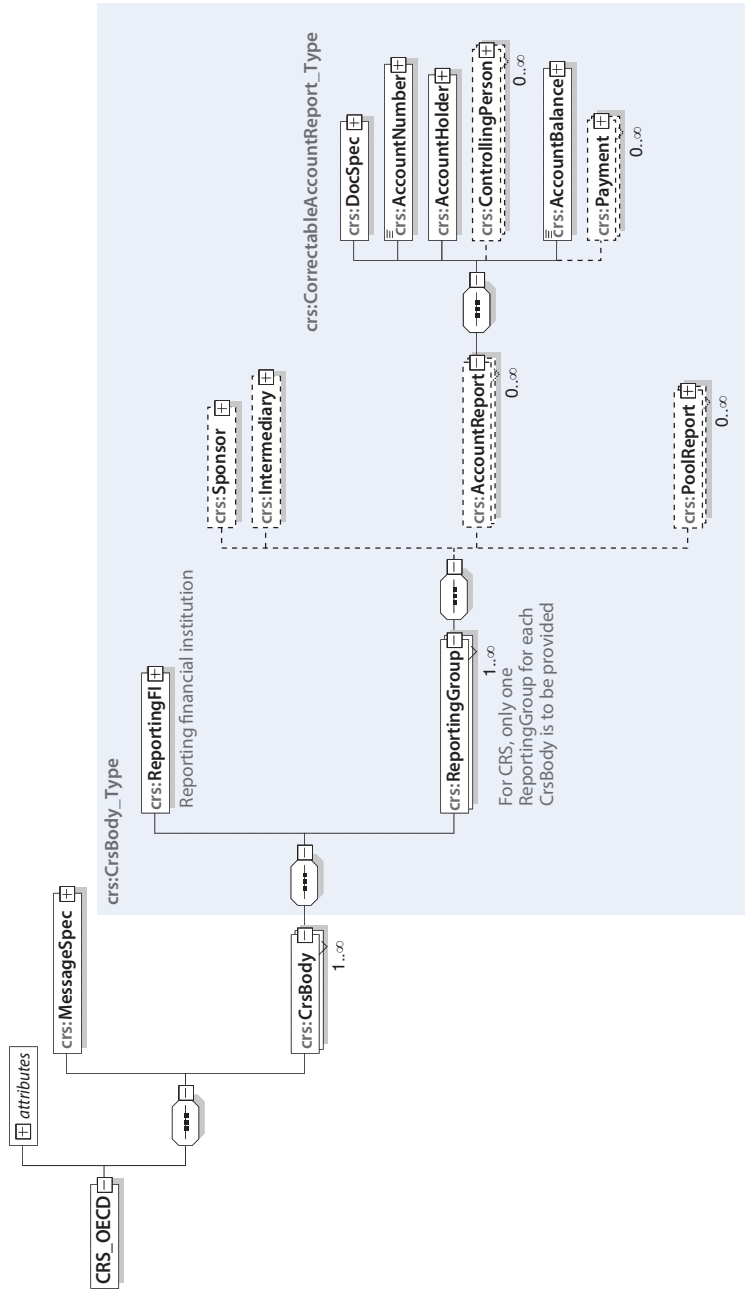
crs:CrsBody
1..∞

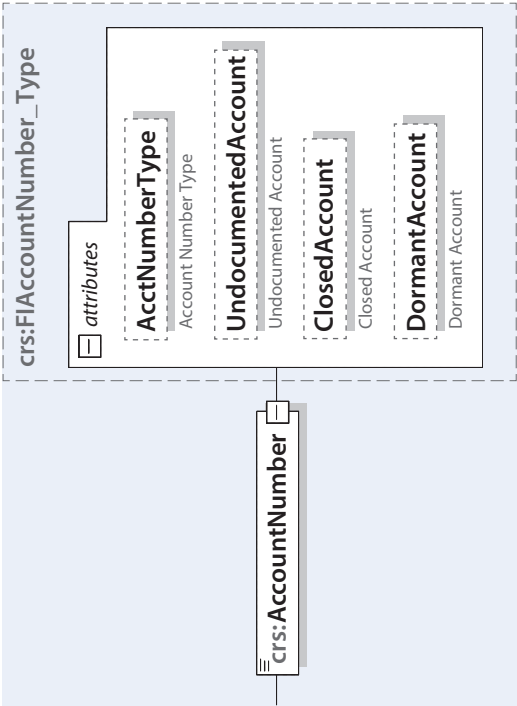# CRS Body (Section IV)

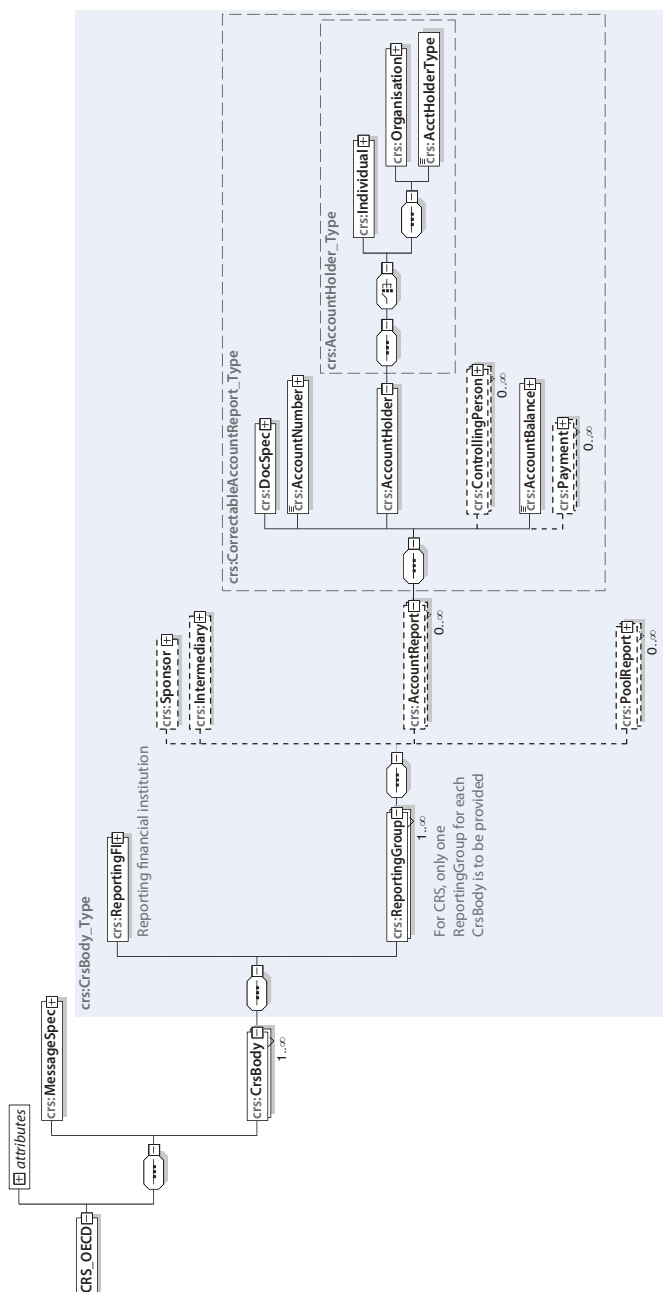## Reporting FI (Section IVa)

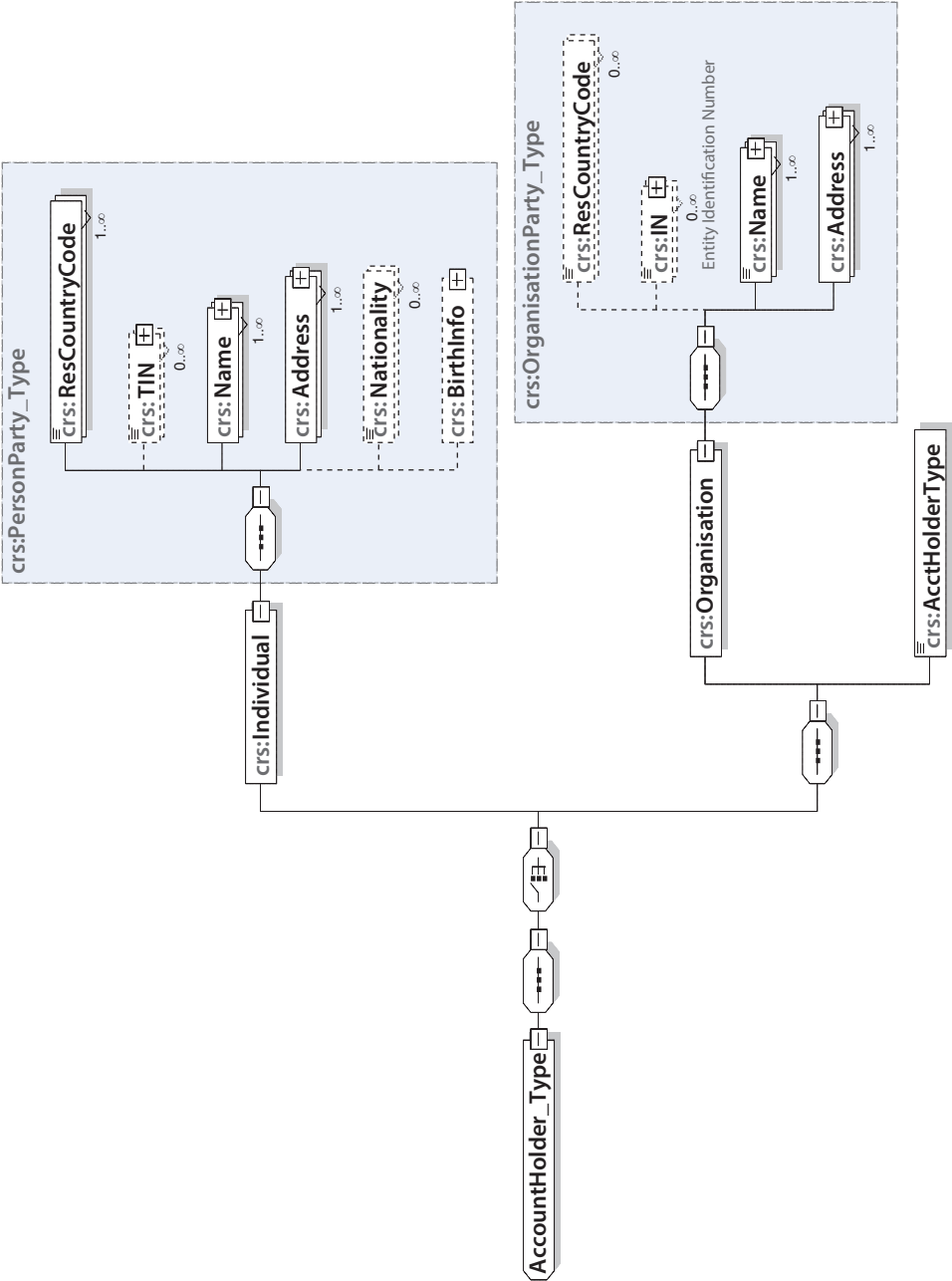## Reporting Group (Section IVb)

Account Report (Section IVc)

Account Number Type (Section IVd)

crs:FIAccountNumber_Type

attributes

AcctNumberType
Account Number Type

UndocumentedAccount
Undocumented Account

ClosedAccount
Closed Account

DormantAccount
Dormant Account

crs:AccountNumber
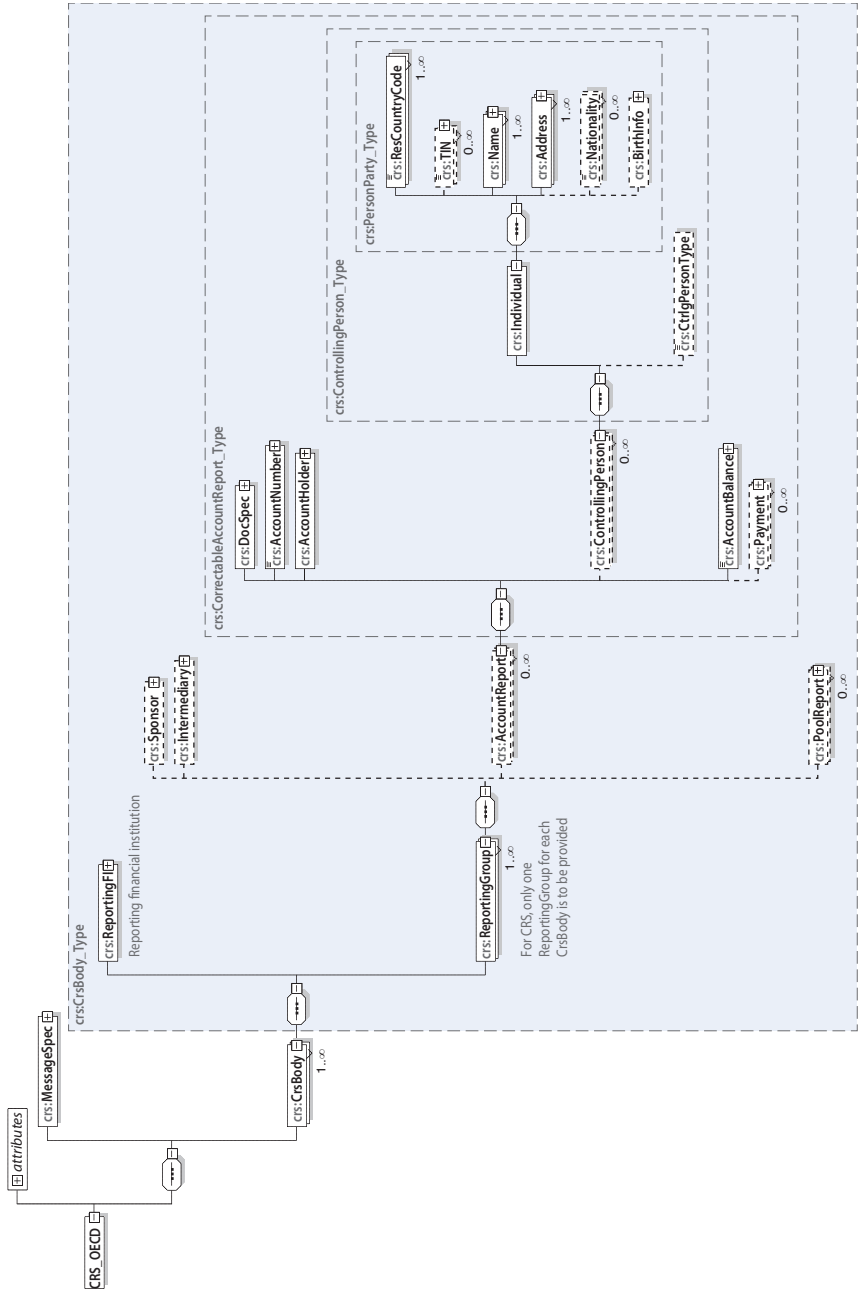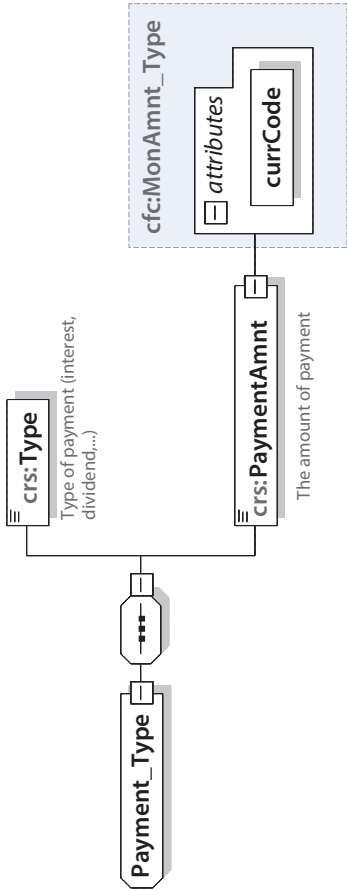
Account Holder (Section IVe)

Individual/Organisation Account Holders (Section IVe)

Controlling Person (Section IVf)

Payment type (Section IVh)

Payment_Type

crs:Type
Type of payment (interest, dividend,....)

crs:PaymentAmnt
The amount of payment

cfc:MonAmnt_Type

attributes

currCode

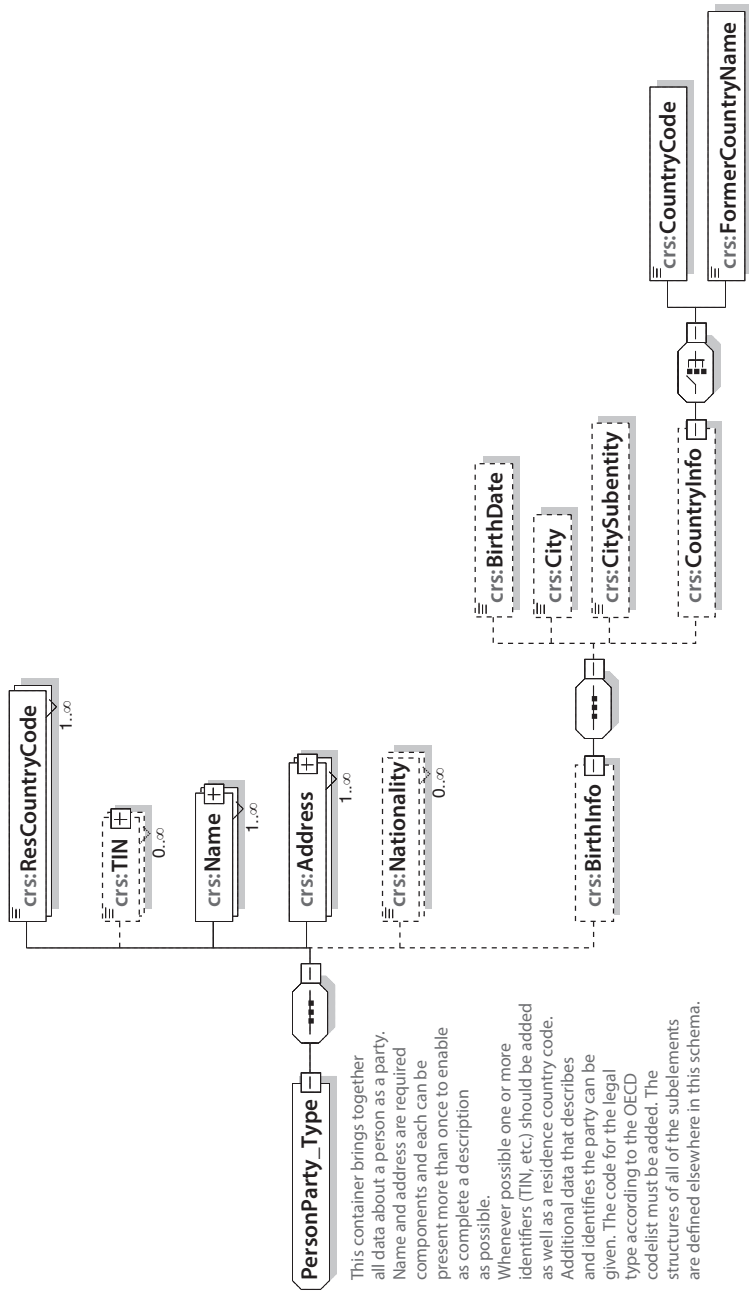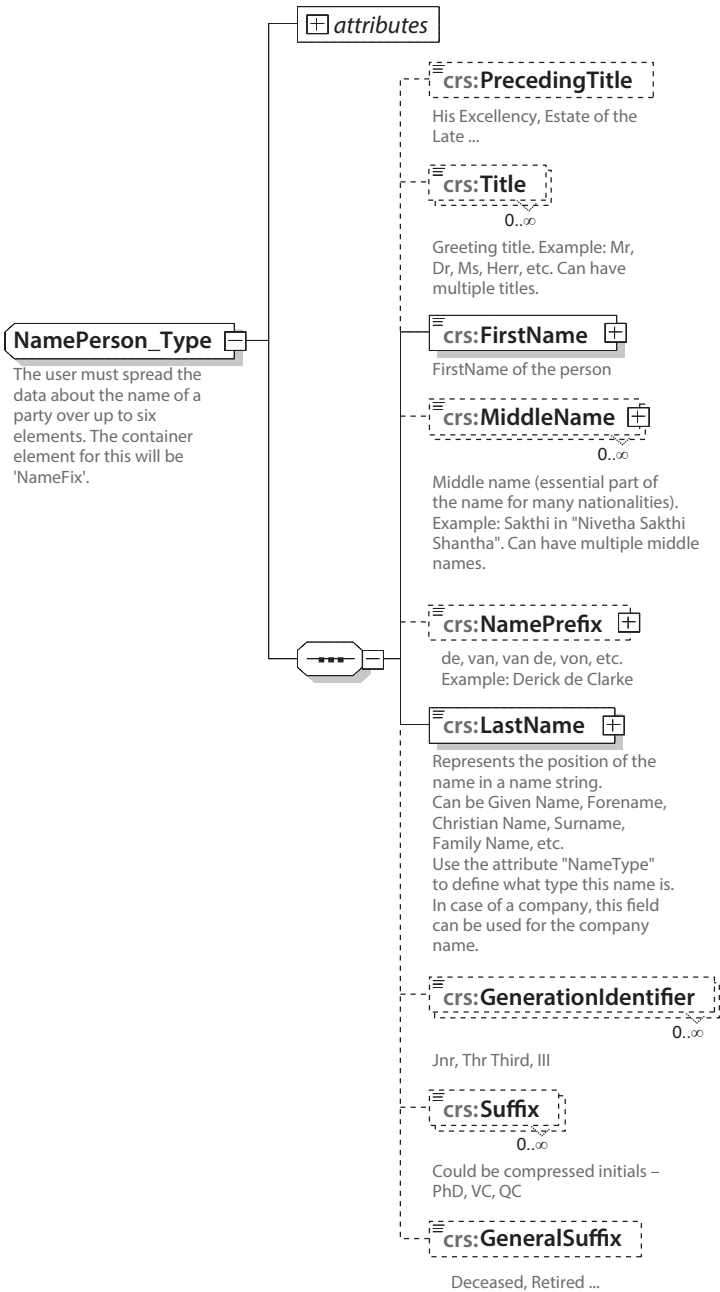*For practical reasons, the CurrencyCode list is based on the ISO 4217 currency code list which is currently used by banks and other financial institutions, and hence by tax administrations. The use of this list does not imply the expression by the OECD of any opinion whatsoever concerning the legal status of the territories listed. Its content is without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.*

Person Party Type (Section II)

PersonParty_Type

This container brings together all data about a person as a party. Name and address are required components and each can be present more than once to enable as complete a description as possible.

Whenever possible one or more identifiers (TIN, etc.) should be added as well as a residence country code. Additional data that describes and identifies the party can be given. The code for the legal type according to the OECD codelist must be added. The structures of all of the subelements are defined elsewhere in this schema.

crs:ResCountryCode
1..∞

crs:TIN
0..∞

crs:Name
1..∞

crs:Address
1..∞

crs:Nationality
0..∞

crs:BirthInfo

crs:BirthDate

crs:City

crs:CitySubentity

crs:CountryInfo

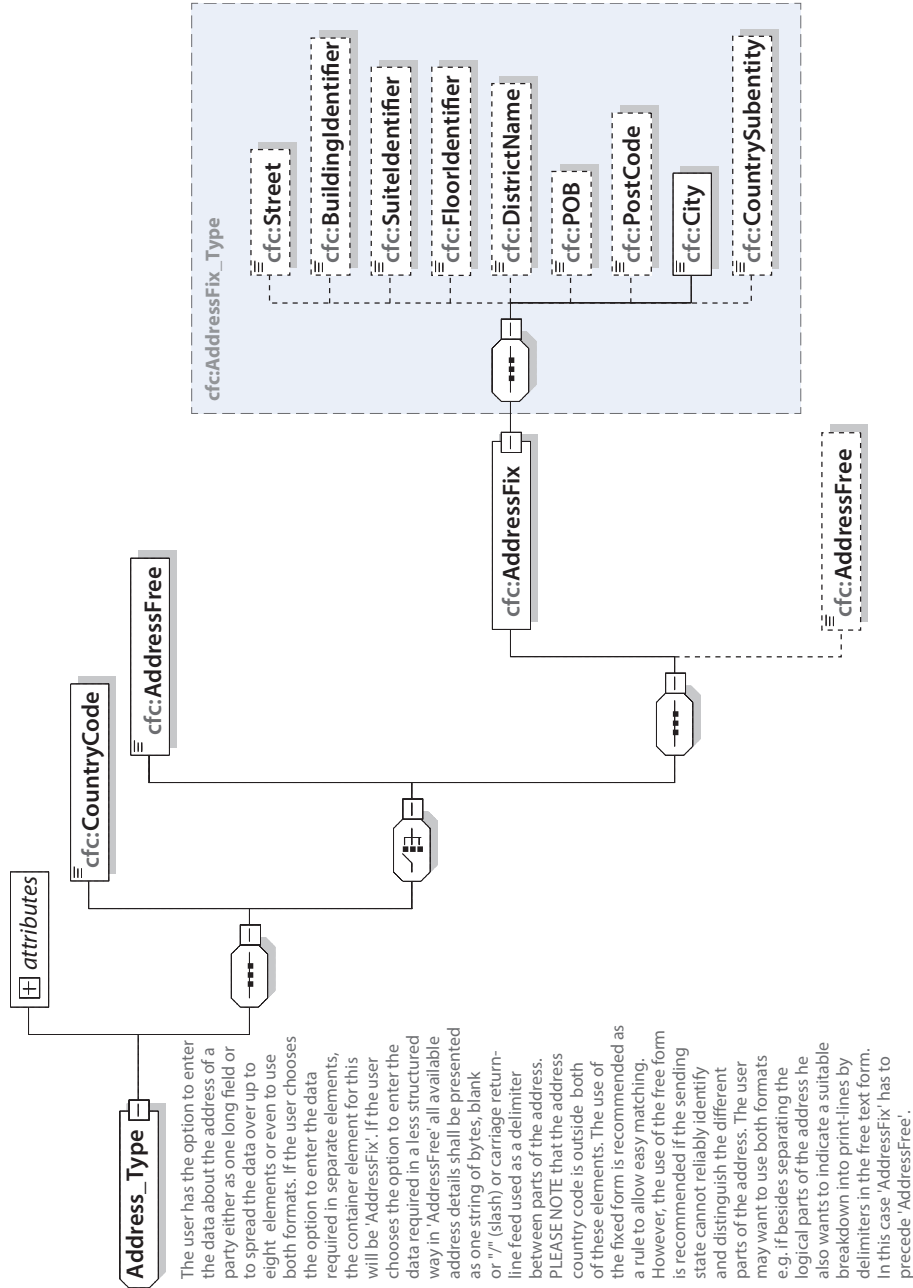**crs:CountryCode**

crs:FormerCountryName

For practical reasons, the ResCountryCode list is based on the ISO 3166-1 country list which is currently used by banks and other financial institutions, and hence by tax administrations. The use of this list does not imply the expression by the OECD of any opinion whatsoever concerning the legal status of the territories listed. Its content is without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.
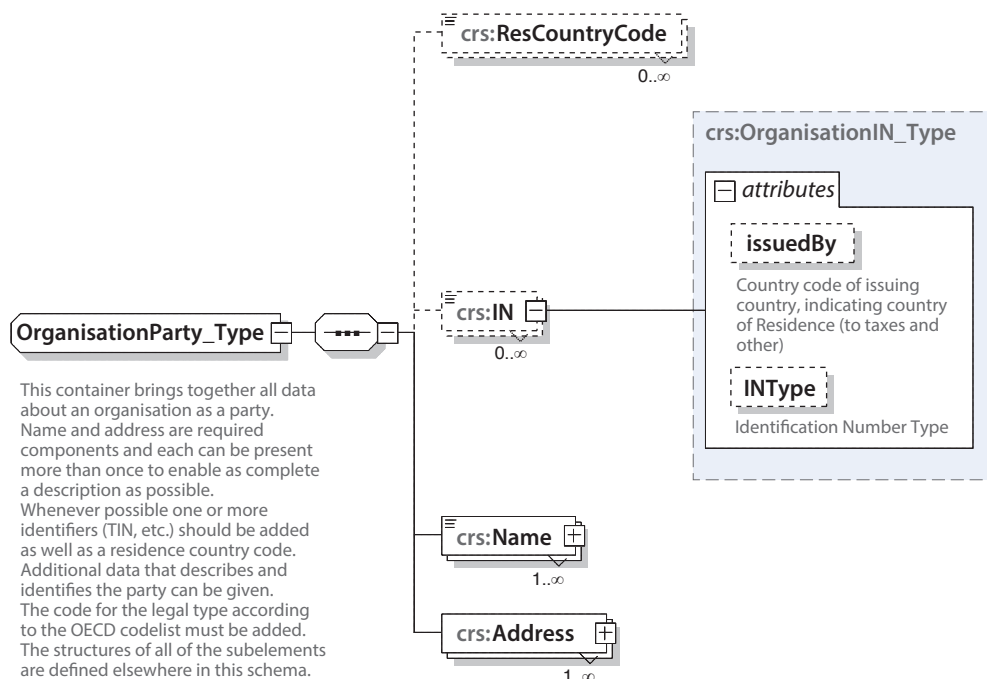
Person Name Type

⊞ *attributes*

crs:PrecedingTitle
His Excellency, Estate of the Late ...

crs:Title
0..∞
Greeting title. Example: Mr, Dr, Ms, Herr, etc. Can have multiple titles.

NamePerson_Type
The user must spread the data about the name of a party over up to six elements. The container element for this will be 'NameFix'.

crs:FirstName ⊞
FirstName of the person

crs:MiddleName ⊞
0..∞
Middle name (essential part of the name for many nationalities). Example: Sakthi in "Nivetha Sakthi Shantha". Can have multiple middle names.

crs:NamePrefix ⊞
de, van, van de, von, etc. Example: Derick de Clarke

crs:LastName ⊞
Represents the position of the name in a name string.
Can be Given Name, Forename, Christian Name, Surname, Family Name, etc.
Use the attribute "NameType" to define what type this name is.
In case of a company, this field can be used for the company name.

crs:GenerationIdentifier
0..∞
Jnr, Thr Third, III

crs:Suffix
0..∞
Could be compressed initials – PhD, VC, QC

crs:GeneralSuffix
Deceased, Retired ...

Address Type

The user has the option to enter the data about the address of a party either as one long field or to spread the data over up to eight elements or even to use both formats. If the user chooses the option to enter the data required in separate elements, the container element for this will be 'AddressFix'. If the user chooses the option to enter the data required in a less structured way in 'AddressFree' all available address details shall be presented as one string of bytes, blank or "/" (slash) or carriage return-line feed used as a delimiter between parts of the address. PLEASE NOTE that the address country code is outside both of these elements. The use of the fixed form is recommended as a rule to allow easy matching. However, the use of the free form is recommended if the sending state cannot reliably identify and distinguish the different parts of the address. The user may want to use both formats e.g. if besides separating the logical parts of the address he also wants to indicate a suitable breakdown into print-lines by delimiters in the free text form. In this case 'AddressFix' has to precede 'AddressFree'.

Organisation Party Type (Section III)

crs:**ResCountryCode**

0..∞

crs:**OrganisationIN_Type**

□ *attributes*

issuedBy

Country code of issuing country, indicating country of Residence (to taxes and other)

INType

Identification Number Type

OrganisationParty_Type

crs:**IN**

0..∞

This container brings together all data about an organisation as a party. Name and address are required components and each can be present more than once to enable as complete a description as possible. Whenever possible one or more identifiers (TIN, etc.) should be added as well as a residence country code. Additional data that describes and identifies the party can be given. The code for the legal type according to the OECD codelist must be added. The structures of all of the subelements are defined elsewhere in this schema.

crs:**Name**

1..∞

crs:**Address**

1..∞

> *For practical reasons, the ResCountryCode list is based on the ISO 3166-1 country list which is currently used by banks and other financial institutions, and hence by tax administrations. The use of this list does not imply the expression by the OECD of any opinion whatsoever concerning the legal status of the territories listed. Its content is without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.*

Pool Report (Non-CRS) (Section IVi)
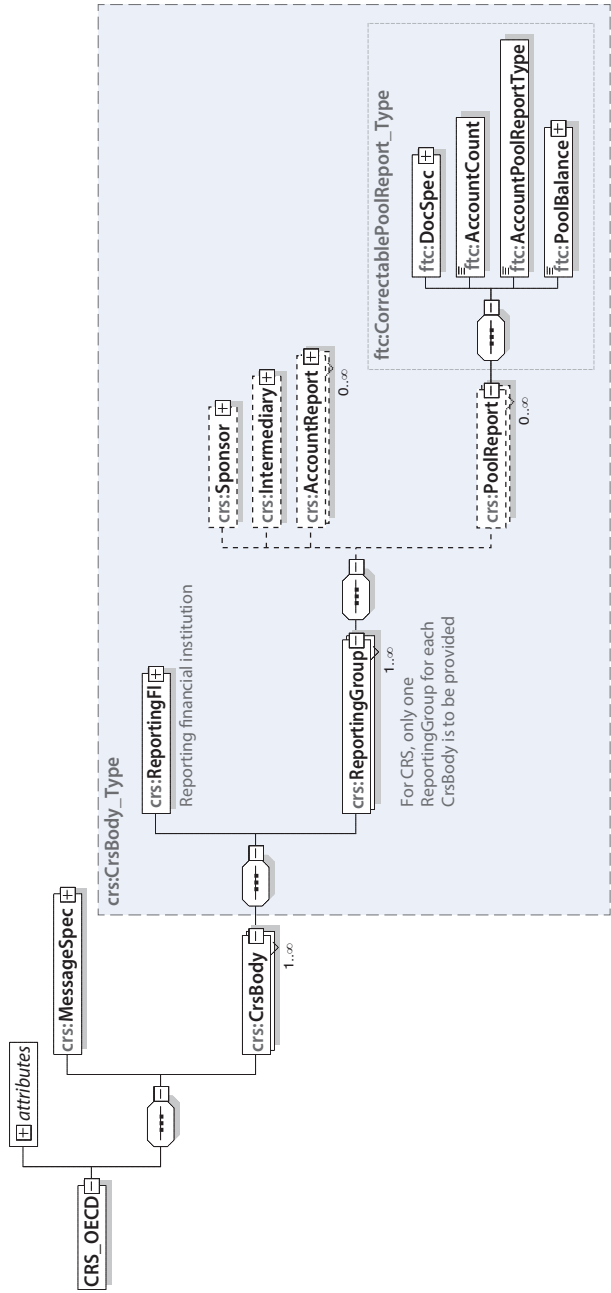
Sponsor & Intermediary (Non-CRS)
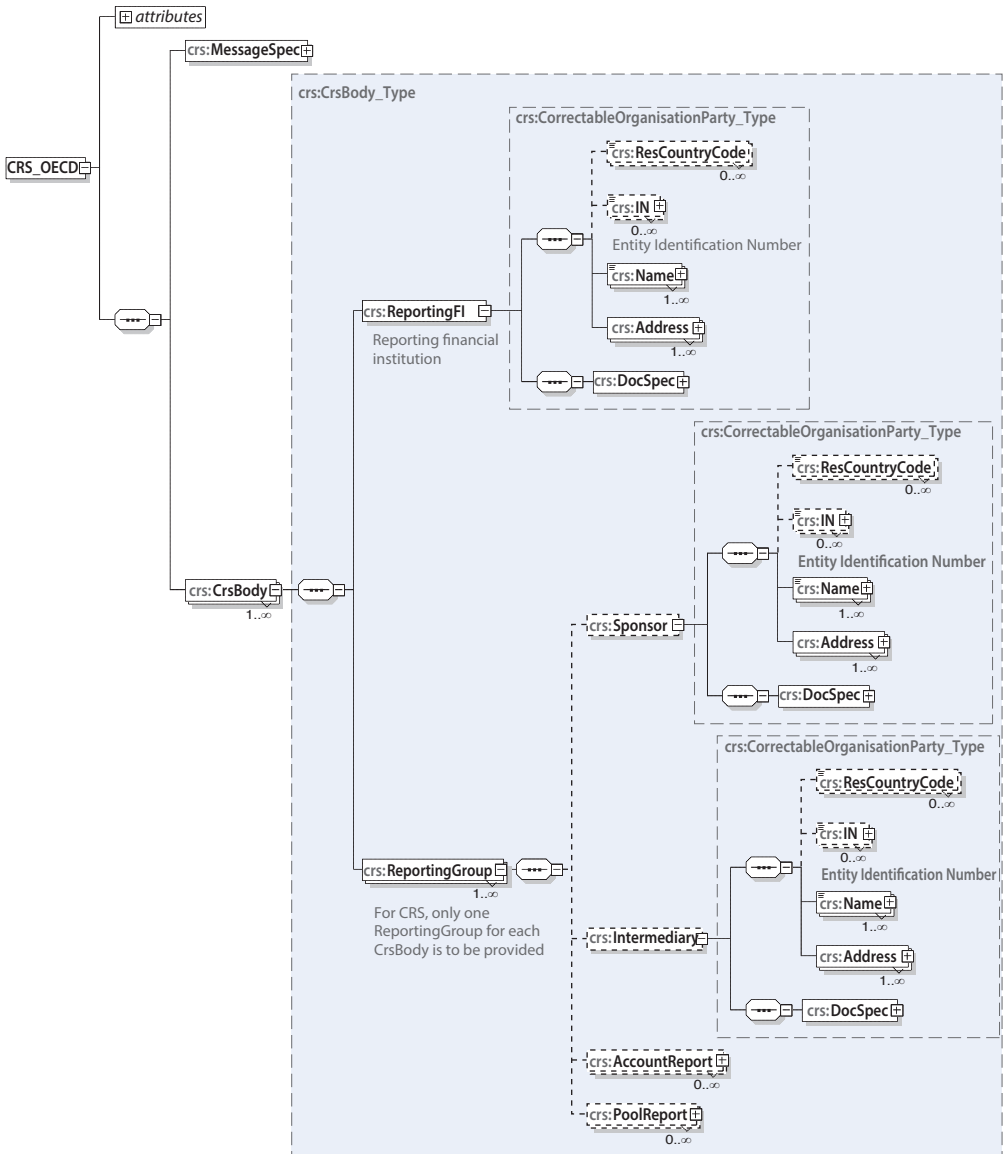
Appendix B

Glossary of Namespaces

CRS Schema Namespaces

Namespace	Description	Filename
crs	CRS specific types	CrsXML_v1.0.xsd
cfc	Common types for FATCA and CRS	CommonTypesFatcaCrs_v1.1.xsd
ftc	FATCA specific types	FatcaTypes_v1.1.xsd
stf	OECD Common Types	OECDTypes_v4.1.xsd
iso	ISO types (Country & Currency codes)	isocrstypes_v1.0.xsd

Annex 4

Example Questionnaire

1. Legal Framework

A legal framework must ensure the confidentiality of exchanged tax information and limit its use to appropriate purposes. The two basic components of such a framework are the terms of the applicable treaty, TIEA or other bilateral agreement for the exchange of information, and a jurisdiction's domestic legislation.

1.1. Tax Conventions, TIEAs & Other Exchange Agreements	
Primary Check-list Areas	• Provisions in tax treaties, TIEAs and international agreements requiring confidentiality of exchanged information and restricting use to intended purposes
How do the exchange of information provisions in your Tax Conventions, TIEAs, or other exchange agreements ensure confidentiality and restrict the use of both outgoing information to other Contracting States and incoming information received in response to a request?	

1.2. Domestic Legislation	
Primary Check-list Areas	• Domestic law must apply safeguards to taxpayer information exchanged pursuant to a treaty, TIEA or other international agreement, and treat those information exchange agreements as binding, restrict data access and use and impose penalties for violations.
How do your domestic laws and regulations safeguard and restrict the use of information exchanged for tax purposes under Tax Conventions, TIEAs, or other exchange instruments? How does the tax administration prevent the misuse of confidential data and prohibit the transfer of tax information from the tax administrative body to non-tax government bodies?	

2. Information Security Management

The information security management systems used by each jurisdiction's tax administration must adhere to standards that ensure the protection of confidential taxpayer data. For example, there must be a screening process for employees handling the information, limits on who can access the information, and systems to detect and trace unauthorised disclosures. The internationally accepted standards for information security are known as the "ISO/IEC 27000-series". As described more fully below, a tax administration should be able to document that it is compliant with the ISO/IEC 27000-series standards or that it has an equivalent information security framework and that taxpayer information obtained under an exchange agreement is protected under that framework.

2.1.1. Background Checks and Contracts	
Primary Check-list Areas	• Screenings and background investigations for employees and contractors • Hiring process and contracts • Responsible Points of Contact
What procedures govern your tax administration's background investigations for employees and contractors who may have access to, use, or are responsible for protecting data received through exchange of information? Is this information publicly available? If so, please provide the reference. If not, please provide a summary of the procedures.	

2.1.2. Training and Awareness	
Primary Check-list Areas	• Initial training and periodic security awareness training based on roles, security risks, and applicable laws
What training does your tax administration provide to employees and contractors regarding confidential information including data received from partners through the Exchange of Information? Does your tax administration maintain a public version of the requirements? If so, please provide the reference. If not, please provide a summary of the requirement.	

2.1.3. Departure Policies	
Primary Check-list Areas	• Departure policies to terminate access to confidential information
What procedures does your tax administration maintain for terminating access to confidential information for departing employees and consultants? Are the procedures publicly available? If so, please provide the reference. If not, please provide a summary of the procedures.	

2.2.1. Physical Security: Access to Premises	
Primary Check-list Areas	• Security measures to restrict entry to premises: security guards, policies, entry access procedures

What procedures does your tax administration maintain to grant employees, consultants, and visitors access to premises where confidential information, paper or electronic, is stored? Are the procedures publicly available? If so, please provide the reference. If not, please provide a summary of the procedures.

2.2.2. Physical Security: Physical Document Storage	
Primary Check-list Areas	• Secure physical storage for confidential documents: policies and procedures

What procedures does your tax administration maintain for receiving, processing, archiving, retrieving and disposing of hard copies of confidential data received from taxpayers or exchange of information partners? Does your tax administration maintain procedures employees must follow when leaving their workspace at the end of the day? Are these procedures publicly available? If yes, please provide the reference. If not, please provide a summary.

Does your tax administration have a data classification policy? If so, please describe how your document storage procedures differ for data at all classification levels. Are these procedures publicly available? If yes, please provide the reference. If not, please provide a summary.

2.3. Planning	
Primary Check-list Areas	• Planning documentation to develop, update, and implement security information systems

What procedures does your tax administration maintain to develop, document, update, and implement security for information systems used to receive, process, archive and retrieve confidential information? Are these procedures publicly available? If yes, please provide the reference. If not, please provide a summary.

What procedures does your tax administration maintain regarding periodic Information Security Plan updates to address changes to the information systems environment, and how are problems and risks identified during the implementation of Information Security Plans resolved? Are these procedures publicly available? If yes, please provide the reference. If not, please provide a summary.

2.4. Configuration Management	
Primary Check-list Areas	• Configuration management and security controls

What policies does your tax administration maintain to regulate system configuration and updates? Are the policies publicly available? If yes, please provide the reference. If not, please provide a summary.

2.5. Access Control

Primary Check-list Areas	• Access Control Policies and procedures: authorised personnel and international exchange of information

What policies does your tax administration maintain to limit system access to authorised users and safeguard data during transmission when received and stored? Please describe how your tax administration's access authorisation and data transmission policies extend to data received from an exchange of information partner under a Treaty or TIEA or other exchange agreement. Are the policies publicly available? If yes, please provide the reference. If not, please provide a summary.

2.6. Identification and Authentication

Primary Check-list Areas	• Authenticating the identifying users and devices that require access to information systems

What policies and procedures does your tax administration maintain for each information system connected to confidential data? Are the policies and procedures publicly available? If so, please provide a reference. If not, please provide a summary.

What policies and procedures govern the authentication of authorised tax administration users by systems connected to confidential data? Are the policies and procedures publicly available? If so, please provide a reference. If not, please provide a summary.

2.7. Audit and Accountability

Primary Check-list Areas	• Traceable electronic actions within systems • System audit procedures: monitoring, analysing, investigating and reporting of unlawful/unauthorised use

What policies and procedures does your tax administration maintain to ensure system audits take place that will detect unauthorised access? Are the policies publicly available? If so, please provide a reference. If not, please provide a summary.

2.8. Maintenance

Primary Check-list Areas	• Periodic and timely maintenance of systems • Controls over: tools, procedures, and mechanisms for system maintenance and personnel use

What policies govern effective periodic system maintenance by your tax administration? Are these policies publicly available? If so, please provide a reference. If not, please provide a summary.

What procedures govern the resolution of system flaws identified by your tax administration? Are these procedures publicly available? If so, please provide a reference. If not, please provide a summary.

2.9. System and Communications Protection

Primary Check-list Areas	• Procedures to monitor, control, and protect communications to and from information systems

What policies and procedures does your tax administration maintain for the electronic transmission and receipt of confidential data. Please describe the security and encryption requirements addressed in these policies. Are these policies publicly available? If so, please provide a reference. If not, please provide a summary.

2.10. System and Information Integrity

Primary Check-list Areas	• Procedures to identify, report, and correct information system flaws in a timely manner • Protection against malicious code and monitoring system security alerts

What procedures does your tax administration maintain to identify, report, and correct information system flaws in a timely manner? Please describe how these procedures provide for the protection of systems against malicious codes causing harm to data integrity. Are these procedures publicly available? If so, please provide a reference. If not, please provide a summary.

2.11. Security Assessments

Primary Check-list Areas	• Processes used to test, validate, and authorise the security controls for protecting data, correcting deficiencies, and reducing vulnerabilities

What policies does your tax administration maintain and regularly update for reviewing the processes used to test, validate, and authorise a security control plan? Is the policy publicly available? If so, please provide a reference. If not, please provide a summary.

2.12. Contingency Planning

Primary Check-list Areas	• Plans for emergency response, backup operations, and post-disaster recovery of information systems

What contingency plans and procedures does your tax administration maintain to reduce the impact of improper data disclosure or unrecoverable loss of data? Are the plans and procedures publicly available? If so, please provide a reference. If not, please provide a summary.

2.13. Risk Assessment

Primary Check-list Areas	• Potential risk of unauthorised access to taxpayer information • Risk and magnitude of harm from unauthorised use, disclosure, or disruption of the taxpayer information systems • Procedures to update risk assessment methodologies

Does your tax administration conduct risk assessments to identify risks and the potential impact of unauthorised access, use, and disclosure of information, or destruction of information systems? What procedures does your tax administration maintain to update risk assessment methodologies? Are these risk assessments and policies publicly available? If so, please provide a reference. If not, please provide a summary.

2.14. Systems and Services Acquisition	
Primary Check-list Areas	• Methods and processes to ensure third-party providers of information systems process, store, and transmit confidential information in accordance with computer security requirements

What process does your tax administration maintain to ensure third-party providers are applying appropriate security controls that are consistent with computer security requirements for confidential information? Are the processes publicly available? If so, please provide a reference. If not, please provide a summary.

2.15. Media Protection	
Primary Check-list Areas	• Processes to protect information in printed or digital form • Security measures used to limit media information access to authorised users only • Methods for sanitising or destroying digital media prior to disposal or reuse

What processes does your tax administration maintain to securely store and limit access to confidential information in printed or digital form upon receipt from any source? How does your tax administration securely destroy confidential media information prior to its disposal? Are the processes available publicly? If so, please provide a reference. If not, please provide a summary.

2.16. Protection of Treaty-Exchanged data	
Primary Check-list Areas	• Procedures to ensure treaty-exchanged files are safeguarded and clearly labeled • Classification methods of treaty-exchanged files

What policies and processes does your tax administration maintain to store confidential information and clearly label it as treaty-exchanged after receipt from foreign Competent Authorities? Are these policies and processes publicly available? If so, please provide a reference. If not, please provide a summary.

2.17. Information Disposal Policies	
Primary Check-list Areas	• Procedures for properly disposing paper and electronic files

What procedures does your tax administration maintain for the disposal of confidential information? Do these procedures extend to exchanged information from foreign Competent Authorities? Are the procedures publicly available? If so, please provide a reference. If not, please provide a summary.

3. Monitoring and Enforcement

In addition to keeping treaty-exchanged information confidential, tax administrations must be able to ensure that its use will be limited to the purposes defined by the applicable information exchange agreement. Thus, compliance with an acceptable information security framework alone is not sufficient to protect treaty-exchanged tax data. In addition, domestic law

must impose penalties or sanctions for improper disclosure or use of taxpayer information. To ensure implementation, such laws must be reinforced by adequate administrative resources and procedures.
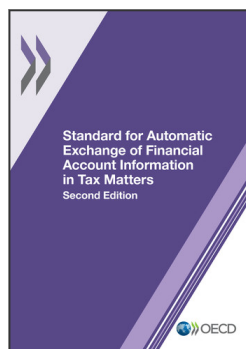
3.1. Penalties and Sanctions	
Primary Check-list Areas	• Penalties imposed for unauthorised disclosures • Risk mitigation practices
Does your tax administration have the ability to impose penalties for unauthorised disclosures of confidential information? Do the penalties extend to unauthorised disclosure of confidential information exchanged with a treaty or TIEA partner? Are the penalties publicly available? If so, please provide a reference. If not, please provide a summary.	

3.2.1. Policing Unauthorised Access and Disclosure	
Primary Check-list Areas	• Monitoring to detect breaches • Reporting of breaches
What procedures does your tax administration have to monitor confidentiality breaches? What policies and procedures does your tax administration have that require employees and contractors to report actual or potential breaches of confidentiality? What reports does your tax administration prepare when a breach of confidentiality occurs? Are these policies and procedures publicly available? If so, please provide a reference. If not, please provide a summary.	

3.2.2. Sanctions and Prior Experience	
Primary Check-list Areas	• Prior unauthorised disclosures • Policy/process modifications to prevent future breaches
Have there been any cases in your jurisdiction where confidential information has been improperly disclosed? Have there been any cases in your jurisdiction where confidential information received by the Competent Authority from an exchange of information partner has been disclosed other than in accordance with the terms of the instrument under which it was provided? Does your tax administration or Inspector General make available to the public descriptions of any breaches, any penalties/sanctions imposed, and changes put in place to mitigate risk and prevent future breaches? If so, please provide a reference. If not, please provide a summary.	