GLOBAL FORUM ON
TRANSPARENCY AND EXCHANGE OF INFORMATION FOR TAX PURPOSES

Terms of Reference for the Confidentiality and Data Safeguards Assessment

OECD
BETTER POLICIES FOR BETTER LIVES

Terms of Reference for the Confidentiality and Data Safeguards Assessment

The confidentiality and data safeguarding requirements of the AEOI Standard

1. Core Requirement 3 of the AEOI peer reviews provides that "jurisdictions should keep the information exchanged confidential and properly safeguarded, and use it in accordance with the exchange agreement under which it was exchanged."[1] A jurisdiction must meet this requirement in order for it to be able to receive information (i.e. to be considered an "Appropriate Partner" to receive information).

2. The requirements are contained, within the AEOI Standard, in Section 5 of the Model Competent Authority Agreement (Model CAA) and its Commentary. Section 7 recognises the importance of maintaining compliance with such requirements and envisages the ability of Competent Authorities to suspend automatic exchanges of information in the case of non-compliance.

3. The elements of Core Requirement 3 are: (i) a legal framework that ensures the confidentiality and appropriate use of exchanged information in accordance with international legal instruments (**Core Requirement 3.1**);[2] (ii) an information security management (ISM) system that adheres to internationally recognised standards or best practices (**Core Requirement 3.2**);[3] and (iii) enforcement provisions and processes to address the occurrence of confidentiality breaches and misuse of information (**Core Requirement 3.3**).[4] These unfold into nine sub-requirements (SR) for the assessments.

4. The aim of the assessments is to provide assurance that jurisdictions keep information confidential and properly safeguarded. To achieve this, it is necessary to protect the information throughout its lifecycle. Jurisdictions may manage the information lifecycle in different ways at the operational level. The operational scope of assessments, particularly by reference to Core Requirements 3.2 and 3.3 may therefore vary from jurisdiction to jurisdiction. Jurisdictions must outline their processes to manage data and the lifecycle of exchanged information at the outset of the assessments to ensure the proper scope of operations is assessed. The assessments may be relied upon by bodies charged with the monitoring and review of the implementation of standards on exchange of information for tax purposes other than the AEOI Standard, in order to minimize overall assessment costs and create efficiencies.[5] Jurisdictions should

[1] *The framework for the second round of AEOI peer reviews, Annex A, The AEOI Terms of Reference* [CTPA/GFTEI(2022)5/FINAL]

[2] Paragraphs 8-10 of the Commentary on Section 5 of the Model CAA

[3] Paragraphs 11-12 of the Commentary on Section 5 of the Model CAA. An ISM system is a set of policies, practices and procedures concerned with information security management, including IT related risks. Internationally recognised standards or best practices in ISM refers to the “ISO/IEC 27000-series”, published jointly by the International Organisation for Standardisation (ISO) and the International Electro-technical Commission (IEC), or to another equivalent standard, or to a jurisdiction’s ISM framework that is equivalent to such standards.

[4] Paragraphs 34-37 of the Commentary on Section 5 of the Model CAA.

[5] As of October 2024, such bodies include only the Inclusive Framework on BEPS with respect to its transparency-related standards, as reflected in the following documents: OECD (2017), BEPS Action 5 on Harmful Tax Practices – “Terms of Reference and Methodology for the Conduct of the Peer Reviews of the Action 5

therefore outline the processes and lifecycle of information exchanged with respect to such other standards, where applicable, to the extent they differ from those of information exchanged under the AEOI Standard.

Transparency Framework", OECD/G20 Base Erosion and Profit Shifting Project, OECD, Paris. www.oecd.org/tax/beps/beps-action-5-harmful-tax-practices-peer-review-transparency-framework.pdf, Methodology at paragraph 7; OECD (2017), "Terms of reference for the conduct of peer reviews of the Action 13 minimum standard on Country-By-Country Reporting" in BEPS Action 13 on Country-by-Country Reporting – Peer Review Documents, OECD/G20 Base Erosion and Profit Shifting Project, OECD, Paris. www.oecd.org/tax/beps/beps-action-13-on-country-by-country-reporting-peer-review-documents.pdf, Methodology at paragraph 7.

Core Requirement 3.1: Jurisdictions should have a legal framework that ensures the confidentiality and appropriate use of information exchanged under an international exchange agreement

SR 3.1.1: Jurisdictions' domestic legal framework should include provisions sufficient to protect the confidentiality of taxpayer information, including treaty-exchanged information, and provide only for specific and limited circumstances under which such information can be accessed, disclosed and used, such circumstances being consistent, in relation to treaty-exchanged information, with the terms of the applicable international exchange instrument (bilateral or multilateral) under which the information was exchanged

Core Requirement 3.2: Jurisdictions should have an Information Security Management (ISM) framework that adheres to internationally recognised standards or best practices and ensures the protection of treaty-exchanged information

5. Tax authorities[6] that are authorised to access information exchanged in accordance with paragraph 2 of Article 22 of the Convention on Mutual Administrative Assistance in Tax Matters or equivalent provisions in other international exchange agreements must have an ISM policy and systems to ensure that information can be used solely for intended purposes and to prevent disclosure to unauthorised persons. An ISM system is a set of governance arrangements, policies, procedures and practices concerned with information security risks, including IT related risks. ISM systems must adhere to internationally recognised standards or best practices.

6. The internationally accepted standards for information security are known as the "ISO/IEC 27000-series," which are published jointly by the International Organisation for Standardisation (ISO) and the International Electro-technical Commission (IEC), though other equivalent standards are also widely recognised and followed by organisations worldwide. Such standards provide best practices on information security management, risks, and controls within the context of an overall ISM system. A tax authority should be able to demonstrate that it has an information security framework that is consistent with the ISO 27000-series or with another equivalent standard, or that it has an equivalent framework.

7. The AEOI Standard specifies that internationally recognised standards or best practices would include a series of baseline (i.e. minimum) ISM controls to be in place.[7] These specific references to baseline controls need to be supplemented by the Standard's general reference to internationally recognised standards or best practices, to ensure that all relevant elements of those standards or best practices are covered. Certain additional elements should be in place, including strategic-level planning and governance arrangements essential to an ISM system. Tax authorities should also have security controls commensurate with their specific AEOI architecture and information security risks.

[6] The term "tax authority" is understood to include tax administrations as well as other authorities charged with processing treaty-exchanged information, e.g. authorities in non-reciprocal jurisdictions with respect to the AEOI Standard that process data with respect to the Standard and do not administer taxes.

[7] Paragraphs 12 and 13-34 of the Commentary on Section 5 of the Model CAA.

8. Tax authorities must meet the ISM requirements in their overall ISM system (SR 3.2.1), in their implementation of various security controls (SR 3.2.2 to 3.2.5), and in their operational framework to test the effectiveness of these controls (SR 3.2.6), as follows:

SR 3.2.1: Tax authorities should have an appropriate overall Information Security Management system

9. Tax authorities should:

   1. display a clear understanding of the lifecycle of treaty-exchanged information within the organisation, be committed to safeguard its confidentiality and appropriate use in line with the applicable international exchange instrument, and have appropriate processes for handling such information (including to maintain awareness of its treaty-exchanged nature);

   2. manage information security through the medium of a written information security policy and appropriate governance and operational arrangements as part of an overarching security framework that clearly defines security roles, responsibilities and reporting lines, is owned by senior management, and is kept up to date;

   3. make security an integral part of the management of the IT environment and IT services, including having in place a change management process with security integrated into it and utilising service level agreements;

   4. systematically manage their information security risks, including risks related to IT, cyber security and treaty-exchanged information, taking account of the threats, vulnerabilities, impacts and security operations management; and

   5. have appropriate arrangements to manage and maintain business and IT service continuity.

SR 3.2.2: Tax authorities should have appropriate human resources controls

10. Tax authorities should:

   1. undertake background checks with appropriate vetting of all candidates for employment, employees, and contractors, in accordance with accepted best practices and perceived risks;

   2. ensure that security roles and responsibilities of employees and contractors are defined, documented, clearly communicated and understood by them, and regularly reviewed, that they receive regular and up-to-date security training and awareness (with those in sensitive roles receiving additional guidance relevant to the handling of more sensitive material), and that they apply security policies and procedures; and

   3. have policies and processes relating to the termination of engagement (including moves to different roles) that protect sensitive information.

SR 3.2.3: Tax authorities should have appropriate physical security arrangements

11. Tax authorities should:

   1. have appropriate physical security plans, policies or other documentation; and protect physical premises, including through internal and external secure perimeters and access controls in relation to employees, visitors and contractors.

SR 3.2.4: Tax authorities should have appropriate IT System Security

12. Tax authorities should:

1. adequately manage their IT assets throughout their lifecycle;

2. deploy an appropriate range of IT security controls, including controls in relation to endpoints (workstations and other devices), servers, infrastructure, applications, software and internet access; and

3. implement logical access controls in line with the 'need to know' and 'least privileged access' principles and based on a logical access policy owned by senior management.

SR 3.2.5: Tax authorities should appropriately protect information

13. Tax authorities should:

1. effectively manage information, including treaty-exchanged information in accordance with a set of policies and procedures throughout the information management lifecycle, including document naming, classification, handling, sharing, storage, retention, and destruction.

SR 3.2.6: Tax authorities should have an appropriate operations management framework, including monitoring, alerting and logging, vulnerability management, incident management and audit

14. Tax authorities should:

1. have appropriate monitoring, alerting and logging arrangements in place, including to detect unauthorised access, use or disclosure of information;

2. have processes and procedures for the identification and management of threats and vulnerabilities;

3. have an incident management system that covers all types of security incidents; and

4. have appropriate internal/external audit functions with respect to information security.

Core Requirement 3.3: Jurisdictions should have enforcement provisions and processes to address confidentiality breaches

SR 3.3.1: Jurisdictions should impose appropriate penalties and/or sanctions for improper access, use or disclosure of information

15. Jurisdictions’ domestic legal framework should enable the imposition of significant penalties and/or sanctions for improper access, disclosure or use of taxpayer information, including treaty-exchanged information, with an appropriate consideration of administrative, civil, and criminal penalties or sanctions.

SR 3.3.2: Jurisdictions should apply appropriate processes to deal with suspected or actual non-compliance, including effectively applying penalties or sanctions

16. Jurisdictions should:

1. have processes to follow when there is suspected or actual unauthorised access, use or disclosure (e.g. identified via incident management or other channels), which should ensure that

such issues are reported and investigated and that appropriate remedial action, including penalties or sanctions and measures to prevent similar future breaches, are applied; and

2. apply processes to notify other Competent Authorities of breaches of confidentiality or failure of safeguards, and of sanctions and remedial actions consequently imposed.