GLOBAL FORUM ON
TRANSPARENCY AND EXCHANGE OF INFORMATION FOR TAX PURPOSES

Confidentiality and Information Security Management Toolkit

OECD
BETTER POLICIES FOR BETTER LIVES

This toolkit was prepared by the Secretariat of the Global Forum on Transparency and Exchange of Information for Tax Purposes.

Table of contents

Abbreviations and acronyms

AEOI	Automatic Exchange of Information
AML	Anti-money laundering
AUP	Acceptable Use Policy
BCM	Business Continuity Management
BCP	Business Continuity Plan
BEPS	Base Erosion and Profit Shifting
BIA	Business Impact Analyses
CCTV	Closed-Circuit TV
CDP	Clean/Clear Desk Policy
CoE	Council of Europe
CMDB	Configuration Management Database
CR	Core Requirement
CRS	Common Reporting Standard
DLP	Data Loss Prevention
DMZ	De-Militarised Zone
DR	Disaster Recovery
DRP	Disaster Recovery Plan
EOI	Exchange of Information
EOIR	Exchange of Information on Request
ETR	Exchange of Tax Rulings
FI	Financial Institution
Global Forum	Global Forum on Transparency and Exchange of Information for Tax Purposes
ISM	Information Security Management
ISO	Information Security Officer
IT	Information Technology
ITSC	Information Technology Service Continuity
MAAC	Convention on Mutual Administrative Assistance in Tax Matters as Amended by the 2010 Protocol
MCAA	Multilateral Competent Authority Agreement
OECD	Organisation for Economic Co-operation and Development
PDCA	Plan; Do; Check; Act
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SOC	Security Operations Centre
SR	Sub-requirement

Preface

Maria José Garde
Chair of the Global Forum

Zayda Manatta
Head of the Global Forum Secretariat

Information confidentiality and security is essential to the relationship between tax administrations and taxpayers around the world. It also underpins the exchange of information in tax matters between governments, one of the pillars of the international taxation system and the multilateral efforts to combat tax evasion and avoidance.

The international community would not have endorsed the Standard for Automatic Exchange of Financial Account Information in Tax Matters, leading to unprecedented global improvement in tax compliance, without its extensive confidentiality and information security management (ISM) requirements.

The Global Forum on Transparency and Exchange of Information for Tax Purposes (Global Forum) has worked since 2014 to monitor, peer review and support members implementing the AEOI Standard. Checking and supporting compliance with the confidentiality requirements has been at the heart of this work.

Collectively, members have taken note of the fact that tax administrations around the world take ISM very seriously. Through the multilateral review and support process, a global picture has emerged of the confidentiality laws and ISM good practices already in place across member jurisdictions, and how their tax administrations incorporate international security standards into their operations.

As we aim to ensure more developing countries can benefit from AEOI, this Confidentiality and ISM toolkit has been developed to offer guidance on the key ISM good practices that form the backbone of the Global Forum's standards in this area.

We hope that all tax administrations, and particularly developing countries aspiring to implement the AEOI Standard and other forms of exchange, will make good use of this guidance to continuously strengthen their handling of exchanged data and other types of data.

About this toolkit

The aim of this Confidentiality and ISM toolkit (the "toolkit") is to assist countries that wish to participate in the automatic exchange of information (AEOI) by ensuring that they meet good practice standards in confidentiality and data safeguarding. It provides general guidance on implementing legal and information security management (ISM) frameworks that ensure the confidentiality of taxpayer information, including information exchanged under international agreements ("exchanged information"), in line with the requirements of the Standard for Automatic Exchange of Financial Account Information in Tax Matters or "AEOI Standard".[1] The implementation of good practice ISM frameworks is also relevant to other types of exchange, such as the exchange of information on request, spontaneous exchange of information, and exchange of Country-by-Country Reports pursuant to the Base Erosion and Profit Shifting (BEPS) Action 13 standard.

The toolkit is divided into four parts, as follows:

- Part 1 offers context on developing countries' participation in AEOI, and introduces the confidentiality and ISM standards by reference to the "Core Requirements" of the Terms of Reference for the Global Forum's confidentiality and data safeguarding peer reviews with respect to the AEOI Standard.
- Part 2 provides guidance to help jurisdictions ensure their legal framework on the confidentiality of taxpayer information is adequate and protects the confidentiality and appropriate use of information exchanged under an international exchange agreement.
- Part 3 presents guidance to help developing countries' tax administrations implement the building blocks of an ISM framework that adheres to internationally recognised standards or best practices, as required by the AEOI Standard. This section is divided into six key areas of ISM ("Sub requirements") into which the Global Forum's requirements are organised.
- Part 4 provides guidance to help jurisdictions and tax administrations ensure that effective enforcement provisions and processes to address confidentiality breaches are in place.

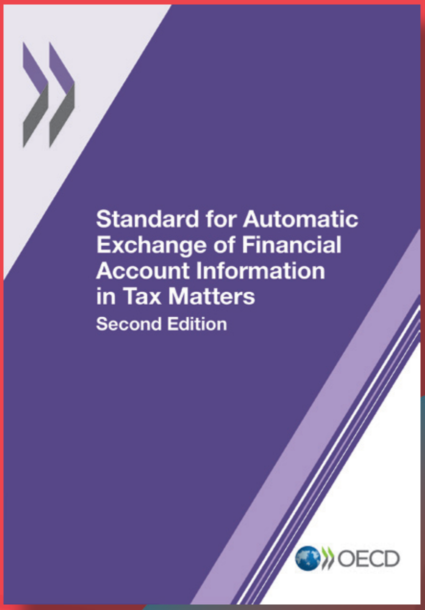
The Annexes contain a glossary of the main concepts covered in the toolkit, as well as useful resources.

[1] www.oecd.org/tax/exchange-of-tax-information/standard-for-automatic-exchange-of-financial-account-information-in-tax-matters-second-edition-9789264267992-en.htm

Disclaimer

This toolkit does not purport to incorporate the elements of internationally recognised ISM standards in an exhaustive manner. Moreover, its contents do not necessarily reflect all possible ways in which a jurisdiction may manage information confidentiality and security consistently with such standards. The toolkit is intended only as a general guide to implementing the building blocks of a confidentiality and ISM framework adapted to tax administrations participating in international information exchanges. It is ultimately for jurisdictions to put in place legal and ISM frameworks suited to their circumstances, on the basis of the particular information confidentiality and security risks that they face.

1. Introduction


Standard for Automatic Exchange of Financial Account Information in Tax Matters
Second Edition
OECD

CONFIDENTIALITY AND DATA SAFEGUARDING AS PILLARS OF TAX INFORMATION EXCHANGE

Taxpayers value the systemic fairness that transparency and exchange of information (EOI) for tax purposes deliver. At the same time, they expect governments exchanging their personal information to treat it with the highest standards of care. The Standard for Automatic Exchange of Financial Account Information in Tax Matters (AEOI Standard),[2] building on the Standard for Exchange of Information on Request (EOIR Standard),[3] therefore 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, and an information security management (ISM) framework that adheres to internationally recognised standards or best practices.

Soon after the AEOI Standard was developed in 2014, the Global Forum endorsed it and put in place a process to deliver its global application, through collective political commitments to implement it within agreed timelines. All Global Forum members, except developing countries that do not host a financial centre, were asked to commit to implement the Standard and commence exchanges with all interested appropriate partners in 2017 or 2018 (defined as those jurisdictions interested in receiving information and that meet the expected confidentiality and data safeguarding requirements). The Global Forum also developed an AEOI peer review mechanism to support, monitor and review implementation of the AEOI Standard.

In this context, the Global Forum put in place a specific process to assess whether jurisdictions committed to AEOI meet the confidentiality and data safeguarding requirements, as a condition to receive data. The assessments are conducted by an expert panel of experienced ISM officials, drawn from peers' tax administrations (coordinated by the Global Forum Secretariat). The confidentiality assessments include:

- A pre exchange assessment before data is received for the first time (commenced in 2015).

[2] Please refer to the Commentary on Section 5, concerning confidentiality and data safeguards, of the Model Competent Authority Agreement within the AEOI Standard: https://read.oecd-ilibrary.org/taxation/standard-for-automatic-exchange-of-financial-account-information-in-tax-matters-second-edition_9789264267992-en#page137

[3] www.oecd.org/tax/transparency/documents/global-forum-handbook-2016.pdf

- A post exchange assessment that gauges the security arrangements for AEOI data after they have been received and are being used (commenced in 2019); and

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

Where weaknesses are identified, jurisdictions are required to make improvements before a satisfactory assessment is concluded and information can be received. If necessary, the Global Forum Secretariat provides technical assistance to help implement the improvements.

Since the compromising of tax administrations' data cannot be entirely ruled out, the Global Forum's processes also include a mechanism to respond to data breaches. This includes re-assessing whether a breached jurisdiction's security arrangements are still fit for purpose, and multilateral communications to inform all relevant stakeholders.

ENSURING DEVELOPING COUNTRIES ALSO BENEFIT FROM AEOI

Global Forum members that are developing countries without a financial centre were not required to implement the AEOI Standard and commence exchanges by 2018. Although these jurisdictions are expected to commit to the Standard in principle as part of their membership obligations, they are encouraged to implement it according to a practicable timeline of their choice (which may be designed with the support of the Global Forum Secretariat).

The Global Forum nevertheless aspires to see the benefits of AEOI being fully extended to developing country members, to improve tax compliance and help mobilise domestic revenues for development. The Secretariat therefore has a capacity building and technical assistance programme in place to help developing countries assess their readiness for AEOI, with confidentiality and data safeguarding as a key pillar of the support provided. In addition to helping members implement the legislative and administrative building blocks of AEOI, the programme aims to help them prepare to meet the requirements of the AEOI Standard and the Global Forum's confidentiality assessment. The programme is outlined in the Global Forum's Plan of Action for Developing Countries' Participation in AEOI.[4]

The programme involves conducting an ISM focused gap analysis of the tax administrations vis-à-vis the confidentiality and data safeguarding requirements for AEOI, and providing technical guidance and project assistance to address the gaps. Available on demand, the assistance programme requires that aspiring members make a firm political commitment to explore a practicable timeline for AEOI, and to then implement it according to that timeline.

A TOOLKIT TO ASSIST DEVELOPING COUNTRY TAX ADMINISTRATIONS' CONFIDENTIALITY AND DATA SAFEGUARDING

While tailored ISM support is provided individually to members upon request, the Global Forum Secretariat has also prepared this toolkit to assist all developing countries' tax administrations put in place, or improve, the key elements of their ISM framework, and securely manage information exchanged under international tax agreements.

The structure of this toolkit follows that of the confidentiality and data safeguards requirements of the AEOI Standard, as incorporated and further detailed in the Terms of Reference for the assessments, and the assessment questionnaire.[5] This will simplify the task for tax administrations carrying out any necessary ISM improvements whilst systematically preparing them for their AEOI confidentiality assessment by the Global Forum.

THE AEOI STANDARD AND THE GLOBAL FORUM'S ASSESSMENT CORE REQUIREMENTS AND SUB-REQUIREMENTS

The AEOI Standard requires jurisdictions to keep the information exchanged confidential and properly safeguarded, and to use it in accordance with the exchange agreement under which it was exchanged. This requirement has been incorporated as Core

[4] www.oecd.org/tax/transparency/documents/plan-of-action-AEOI-and-developing-countries.pdf

[5] The Terms of Reference can be accessed at www.oecd.org/tax/transparency/documents/confidentiality-data-safeguards-assessments-tor.pdf. The confidentiality and data safeguards assessment questionnaire is made available by the Secretariat to jurisdictions' authorised persons upon request.

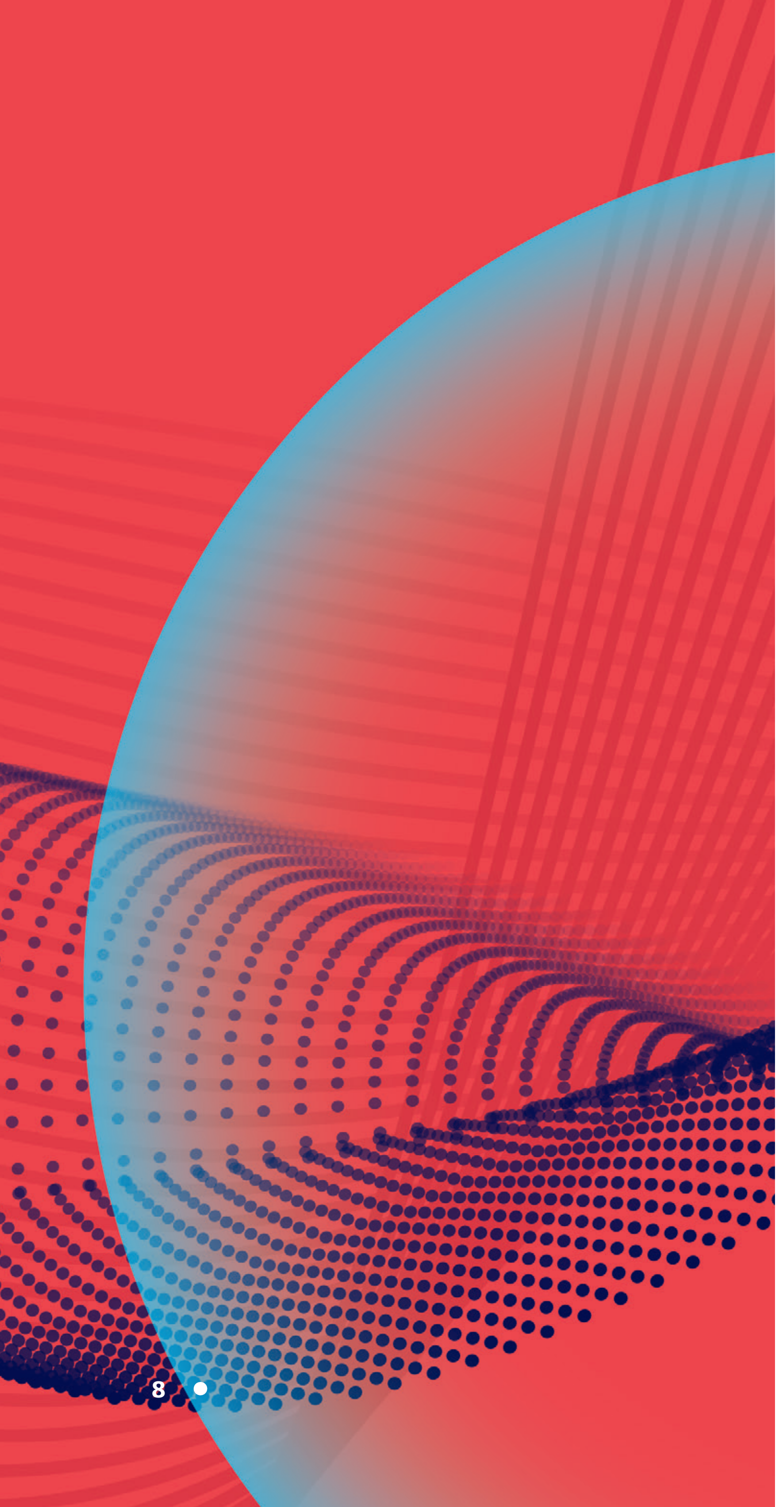
Requirement (CR) 3 in the Terms of Reference for the AEOI peer review process.[6] CR 3 unfolds into three essential building blocks (CRs 1-3) that should be in place, which in turn unfold into Sub-requirements (SR), as shown in Table 1. This toolkit provides guidance on each CR and SR.

Table 1. **Core Requirements and Sub-requirements of the confidentiality assessments**

CR 3.1 Jurisdictions should have a legal framework that ensures the confidentiality and proper use of exchanged information	CR 3.2 Jurisdictions should have an ISM framework that adheres to internationally recognised standards or best practices	CR 3.3 Jurisdictions should have enforcement provisions and processes to address confidentiality breaches
● SR 3.1.1 Juridictions' domestic legal framework should include provisions sufficient to protect the confidentiality of taxpayer information, including exchanged information, and provide only for specific and limited circumstances under which such information can be disclosed and used, such circumstances being consistent, in relation to exchanged information, with the terms of the applicable international exchange instrument (bilateral or multilateral) under which the information was exchanged.	● SR 3.2.1 Relevant organisations should have an appropriate overall Information Security Management system. ● SR 3.2.2 Relevant organisations should have appropriate human resources controls. ● SR 3.2.3 Relevant organisations should have appropriate access controls, including physical and logical access. ● SR 3.2.4 Relevant organisations should have appropriate IT System Security. ● SR 3.2.5 Relevant organisations should appropriately protect information. ● SR 3.2.6 Relevant organisations should have an appropriate operations management framework, including incident management, change management, monitoring and audit.	● SR 3.3.1 Jurisdictions should impose appropriate penalties and/or sanctions for improper use or disclosure of information. ● SR 3.3.2 Jurisdictions should apply appropriate processes to deal with suspected or actual non-compliance, including effectively applying penalties or sanctions.

[6] www.oecd.org/tax/transparency/documents/AEOI-terms-of-reference.pdf. CRs 1 and 2 of the AEOI peer reviews relate to the effective collection and exchange of information with respect to the AEOI Standard. CR 1 requires that jurisdictions ensure that all reporting financial institutions apply due diligence procedures in accordance with the Common Reporting Standard (CRS) to review the financial accounts they maintain, and collect and report the information required. CR 2 requires that jurisdictions exchange the information with all interested appropriate partners, in a timely manner, and ensuring it is collected, sorted, prepared, validated and transmitted in accordance with the AEOI Standard.

2. Legal framework to ensure confidentiality and appropriate use of exchanged information (Core Requirement 3.1)



REQUIREMENTS IN INTERNATIONAL EXCHANGE AGREEMENTS

Effective mutual assistance in tax matters requires each jurisdiction to be assured that the other will treat with proper confidence the information obtained in the course of their co operation.

International exchange agreements therefore contain provisions regarding confidentiality and the obligation for Contracting States, i.e. the exchange partner jurisdictions, to keep exchanged information as secret or confidential, in the same manner as information collected under their domestic laws. Exchange partners may suspend EOI if appropriate safeguards are not in place, or if there has been a breach of confidentiality and they are not satisfied that the situation has been appropriately resolved.

Box 1 shows extracts of various model international exchange provisions in relation to confidentiality, upon which most current international agreements are based. Jurisdictions should seek to include equivalent provisions in new EOI agreements reached with their partners.

A corollary of these international obligations is that the confidentiality of taxpayer information, including exchanged information, should be protected by a domestic legal framework that is enforceable, and that underpins jurisdictions' practical measures to ensure confidentiality.

Absent such framework, exchange partners, as well as taxpayers, will not be assured that confidentiality will be protected and that violations and breaches of confidentiality will be appropriately addressed and sanctioned, even if robust practical ISM measures are in place.

In this context, CR 3.1 requires that jurisdictions have a legal framework that ensures the confidentiality and appropriate use of information exchanged under an international exchange agreement.

Legal framework to ensure confidentiality and appropriate use of exchanged information (Core Requirement 3.1)

Box 1. Confidentiality provisions in model international exchange agreements and the multilateral Convention on Mutual Administrative Assistance in Tax Matters (MAAC)

Article 26(2) of the OECD Model Tax Convention on Income and on Capital[7]

"Any information received under paragraph 1 by a Contracting State shall be treated as secret in the same manner as information obtained under the domestic laws of that State and shall be disclosed only to persons or authorities (including courts and administrative bodies) concerned with the assessment or collection of, the enforcement or prosecution in respect of, the determination of appeals in relation to the taxes referred to in paragraph 1, or the oversight of the above. Such persons or authorities shall use the information only for such purposes. They may disclose the information in public court proceedings or in judicial decisions. Notwithstanding the foregoing, information received by a Contracting State may be used for other purposes when such information may be used for such other purposes under the laws of both States and the competent authority of the supplying State authorises such use."

Article 8 of the OECD Model Agreement on Exchange of Information in Tax Matters[8]

"Any information received by a Contracting Party under this Agreement shall be treated as confidential and may be disclosed only to persons or authorities (including courts and administrative bodies) in the jurisdiction of the Contracting Party concerned with the assessment or collection of, the enforcement or prosecution in respect of, or the determination of appeals in relation to, the taxes covered by this Agreement. Such persons or authorities shall use such information only for such purposes. They may disclose the information in public court proceedings or in judicial decisions. The information may not be disclosed to any other person or entity or authority or any other jurisdiction without the express written consent of the competent authority of the requested Party."

Article 26(2) of the United Nations Model Tax Convention Between Developed and Developing Countries[9]

"Any information received under paragraph 1 by a Contracting State shall be treated as secret in the same manner as information obtained under the domestic laws of that State and it shall be disclosed only to persons or authorities (including courts and administrative bodies) concerned with the assessment or collection of, the enforcement or prosecution in respect of, or the determination of appeals in relation to, the taxes referred to in paragraph 1, or the oversight of the above. Such persons or authorities shall use the information only for such purposes. They may disclose the information in public court proceedings or in judicial decisions. Notwithstanding the foregoing, information received by a Contracting State may be used for other purposes when such information may be used for such other purposes under the laws of both States and the competent authority of the supplying State authorizes such use."

Article 22 (Secrecy) of the MAAC[10]

1. Any information obtained by a Party under this Convention shall be treated as secret and protected in the same manner as information obtained under the domestic law of that Party and, to the extent needed to ensure the necessary level of protection of personal data, in accordance with the safeguards which may be specified by the supplying Party as required under its domestic law.

2. Such information shall in any case be disclosed only to persons or authorities (including courts and administrative or supervisory bodies) concerned with the assessment, collection or recovery of, the enforcement or prosecution in respect of, or the determination of appeals in relation to, taxes of that Party, or the oversight of the above. Only the persons or authorities mentioned above may use the information and then only for such purposes. They may, notwithstanding the provisions of paragraph 1, disclose it in public court proceedings or in judicial decisions relating to such taxes.

3. [...]

4. Notwithstanding the provisions of paragraphs 1, 2 and 3, information received by a Party may be used for other purposes when such information may be used for such other purposes under the laws of the supplying Party and the competent authority of that Party authorises such use. Information provided by a Party to another Party may be transmitted by the latter to a third Party, subject to prior authorisation by the competent authority of the first-mentioned Party.

[7] https://read.oecd-ilibrary.org/taxation/model-tax-convention-on-income-and-on-capital-condensed-version-2017_mtc_cond-2017-en#page47

[8] www.oecd.org/tax/exchange-of-tax-information/2082215.pdf

[9] www.un-ilibrary.org/content/books/9789210474047

[10] https://read.oecd-ilibrary.org/taxation/the-multilateral-convention-on-mutual-administrative-assistance-in-tax-matters_9789264115606-en#page23

Legal framework to ensure confidentiality and appropriate use of exchanged information (Core Requirement 3.1)

International exchange agreements also contain provisions limiting to whom exchanged information can be disclosed and the purposes for which it can be used (see Box 1). Generally, disclosure is limited to persons or authorities (including courts and administrative bodies) involved in the:

- Assessment
- Collection
- Enforcement
- Prosecution, and
- Determination of appeals

in relation to the taxes with respect to which information may be exchanged under the applicable agreement.

Exchanged information may also be communicated to the taxpayer, their proxy or to a witness. It can also be disclosed to governmental or judicial authorities charged with deciding whether such information should be released to the taxpayer, their proxy or to the witnesses. Courts and administrative bodies involved in the tax purposes mentioned above can disclose the information in court sessions or court decisions. Once information is used in public court proceedings or in court decisions and thus rendered public, it is clear that from that moment such information can be quoted from the court files or decisions for other purposes even as possible evidence. But this does not mean that the aforementioned persons and authorities are allowed to provide on request additional information received. If either or both of the exchange partners object to the information being made public by courts in this way, or, once the information has been made public in this way, to the information being used for other purposes, because this is not the normal procedure under their domestic laws, they should state this expressly in their exchange agreement.

In short, agreements providing for EOI in tax matters generally authorise the disclosure and use of exchanged information for tax purposes.

Nonetheless, exchange partners may agree to permit the disclosure and use of information exchanged for tax purposes also for additional purposes, e.g. to assist in the investigation and prosecution of money laundering or terrorist financing offences. In such cases, those other purposes should be consistent with each of the exchange partners' domestic laws, and a jurisdiction that receives information should seek authorisation from the competent authority of the jurisdiction supplying the information to disclose and use it for non tax purposes. The MAAC, notably, provides for this possibility (see Box 1).

In this context, a competent authority(ies) is/are the person(s) or government authority(ies) designated by a jurisdiction as being competent to exchange information pursuant to an international exchange agreement.

SUB-REQUIREMENT 3.1.1: LEGAL FRAMEWORK THAT ENSURES THE CONFIDENTIALITY AND PROPER USE OF INFORMATION EXCHANGED

In view of the confidentiality requirements of international exchange agreements, SR 3.1.1 requires that each jurisdictions' domestic legal framework should include provisions sufficient to protect the confidentiality of taxpayer information, including exchanged information, and provide only for specific and limited circumstances under which such information can be disclosed and used, such circumstances being consistent, in relation to exchanged information, with the terms of the applicable international exchange instrument (bilateral or multilateral) under which the information was exchanged.

There are therefore two key aspects to SR 3.1.1:

- There should be a legal framework protecting the confidentiality of taxpayer information in general, and exchanged information should be within the scope of the legal protection.
- The legal framework should ensure the disclosure and use of exchanged information in limited circumstances, and in line with the terms agreed in the international exchange agreement under which it was exchanged.

Legal framework protecting the confidentiality of taxpayer information, including exchanged information

A jurisdiction's domestic legal framework should provide for the confidentiality or secrecy of taxpayer information, meaning information pertaining to taxpayers in respect of their income, expenditure, accounts, tax liability, personal details, business affairs or other relevant aspects that a tax administration may handle in order to fulfil its functions.

Confidentiality rules may be contained in legislative statutes, secondary or executive regulations, or administrative guidance. Whichever the legislative instrument used, the rules should be legally binding and enforceable.

More specifically, domestic law should:

- Provide that taxpayer information handled by the tax administration is confidential or secret.
- Bind all personnel (including permanent, temporary or contractual personnel) to the utmost secrecy and confidentiality of taxpayer information they may handle in the course of their work.
- Ensure that the confidentiality or secrecy obligations apply to personnel throughout their engagement, and also following the termination of engagement, transfer to other job functions, retirement, end of contract, or similar event bringing their handling of taxpayer information to an end (this aspect is addressed in detail in SR 3.2.2 on human resources controls).
- Provide for penalties or sanctions to deter and punish violations or breaches of confidentiality (penalties and sanctions are addressed in detail in SR 3.3.1).

Box 2. **Examples of what a governing confidentiality provision could cover**

Jurisdiction A's domestic legal framework includes confidentiality provisions that cover tax information across multiple laws. The Income Tax Act imposes a general obligation on all personnel of the tax administration (including contractors) to ensure the confidentiality of any taxpayer information handled in the course of their duties. Further, the Official Secrets Act prohibits the disclosure of any secret information by existing or former public officials or contractors.

Jurisdiction B's Public Employment Law imposes a duty of confidentiality on all public officials (including temporary staff and contractors providing services to public authorities). The Code of Conduct of Public Officials requires the confidentiality of all information they may have access to in the course of their employment. In relation to exchanged information, the International Tax Co-operation Law specifically covers all personnel and contractors working on any aspect of exchange of information (including those engaged to provide IT services) and brings them within the scope of the general tax information confidentiality provisions.

Tax confidentiality rules may be contained in tax laws, in more general laws (e.g. laws governing public employment or civil service duties), privacy or data protection laws, and/or other laws (see Box 2 for examples).

In some jurisdictions, the general provisions on tax information confidentiality may be sufficiently broad so as to cover exchanged information. One example would be a provision contained in tax law that imposes a confidentiality or secrecy obligation on public officials or persons engaged by the tax administration regarding any taxpayer information that they may handle in the course of their duties, irrespective of the source of the information (i.e. domestic source or EOI), and irrespective of whether the taxpayer is a domestic or foreign tax resident.

If the coverage of exchanged information is not ensured by the general provisions, however, jurisdictions will need to enact specific provisions ensuring that the legal protection of confidentiality extends to it.

Appropriate disclosure and use of exchanged information in line with international exchange agreements

Domestic laws in many jurisdictions permit the sharing of taxpayer information with non-tax public authorities. For example, it is not uncommon for laws to enable the disclosure of certain taxpayer information to:

- Investigative and law enforcement agencies such as anti-corruption agencies, anti-money laundering (AML) authorities, or customs authorities.
- Social security authorities for purposes of administering welfare benefits.
- Members of the public in appropriate cases, pursuant to freedom of information rules.

Legal framework to ensure confidentiality and appropriate use of exchanged information (Core Requirement 3.1)

As international exchange agreements generally provide for narrower disclosure and use circumstances, as described in this toolkit, jurisdictions should ensure that the obligations in their exchange agreements are given effect and are binding within the domestic legal framework, so that exchanged information is disclosed and used only as agreed with exchange partners.

Jurisdictions give effect to their international obligations (including confidentiality obligations) in different ways (see Box 3 for examples). One approach is to amend domestic legislation to ensure that international agreement obligations are respected under domestic law. In some jurisdictions, international legal obligations prevail over domestic laws in the event of inconsistency by virtue of statutes on the hierarchy of laws, or the constitution. In other jurisdictions, obligations under international agreements are implemented in such a way that in the event of an inconsistency with domestic law, the agreement overrides it. Some countries use a combination of the two approaches.

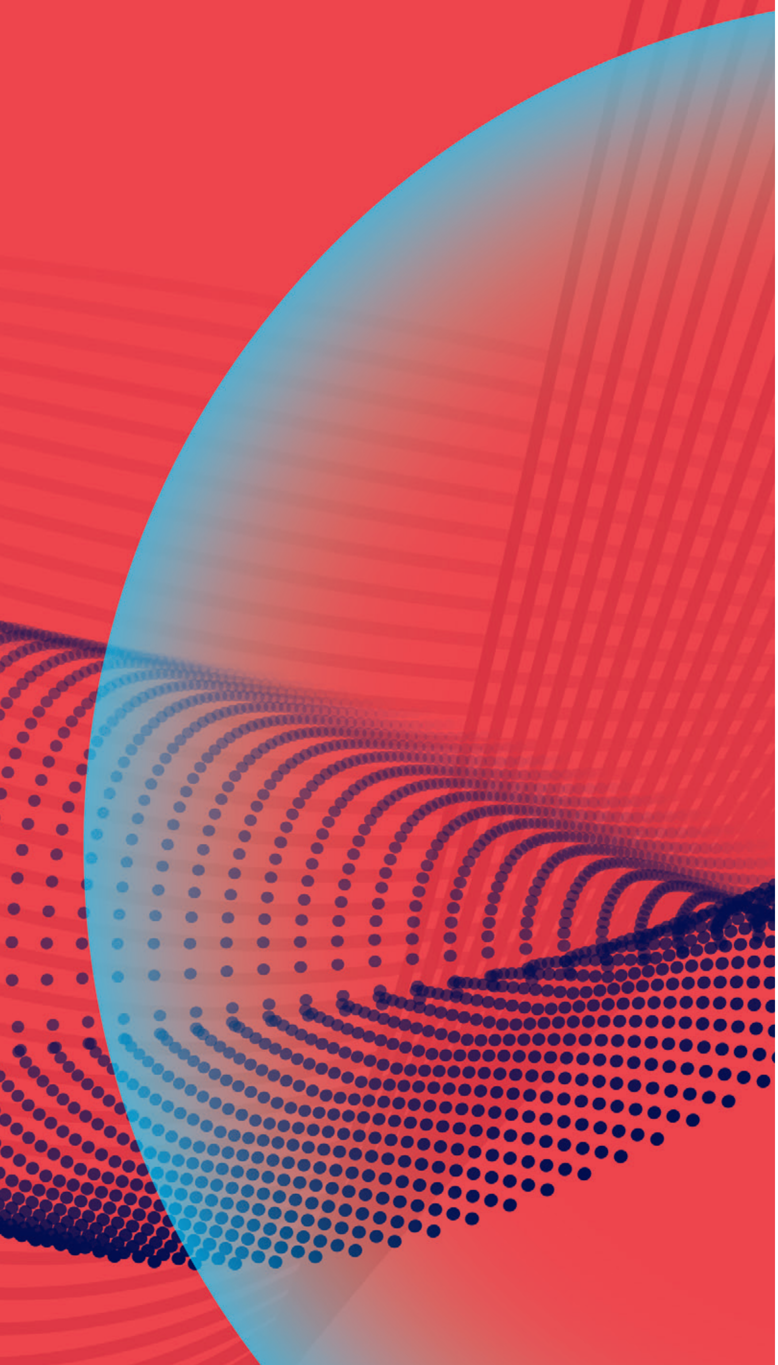
Jurisdictions may supplement the legal rules on disclosure and use of exchanged information with guidance on the procedure to disclose or make use of it for non-tax purposes, where permitted. The guidance can specify the need to seek authorisation from the competent authority of the exchange partner that has provided the information, and to ensure that the disclosure and use is consistent with the laws of both parties.

Box 3. Examples of legislation giving effect to international exchange agreements

In Jurisdiction A, when there are inconsistencies between domestic law and international agreements, the legislation introducing agreements into domestic law makes it clear that the agreement takes precedence.

In Jurisdiction B, there is legislation providing that any restrictions on the use of exchanged information agreed with or imposed by a foreign jurisdiction shall apply even if contrary to domestic law.

3. Information Security Management framework that adheres to internationally recognised standards or best practices (Core Requirement 3.2)



THE NEED FOR AN ISM FRAMEWORK

In order for the legal protections afforded under international agreements and domestic law to be meaningful, practices and procedures must be in place to give them effect. CR 3.2 therefore requires jurisdictions to have an Information Security Management (ISM) framework that adheres to internationally recognised standards or best practices and ensures the protection of exchanged information.

An ISM framework is a set of governance arrangements, policies, procedures, practices and security controls. A security control is a specific measure to mitigate or eliminate a security risk: it could be a procedure, a hardware or software product, or other.

The AEOI Standard contains requirements for a comprehensive ISM framework due to the sensitive nature, large volumes, and electronic means through which the information is exchanged. Thousands of financial account records may flow into tax administrations' systems and be handled by a range of business processes, IT systems and people. These features raise significant security risks, including improper access to information by staff or targeted cyber attacks that may lead to confidentiality breaches if not properly mitigated.

The various controls, within an ISM framework, that are applied to such processes, systems and people tend to reduce the risks and threats to information and create a "culture of care" within a tax administration.

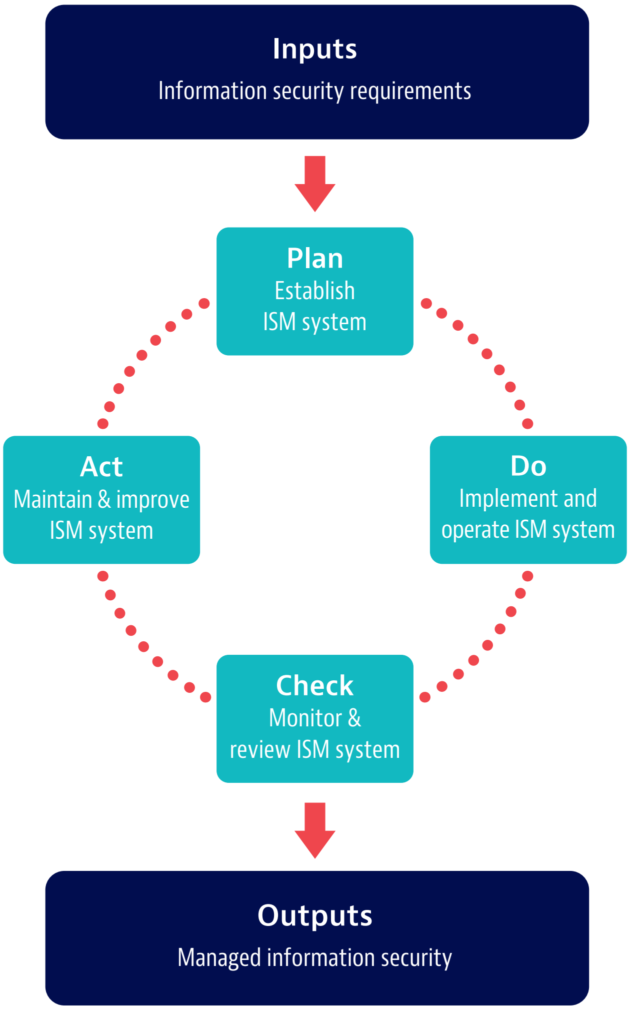
INTERNATIONALLY RECOGNISED STANDARDS OR BEST PRACTICES

Internationally recognised standards or best practices in ISM refer to standards such as the "ISO/IEC 27000-series", published jointly by the International Organisation for Standardisation (ISO) and the International Electro-technical Commission (IEC), or other equivalent standards. Tax administrations worldwide draw on various national or international standards and there is no single, universally accepted ISM standard, although the ISO/IEC 27000 series are the most commonly referenced in the Global Forum's work.

The ISO/IEC 27000 series, although complex in content, may be represented in a simplified form by using the widely recognised, iterative, continuous improvement process represented by the acronym "PDCA", or "Plan; Do;

Information Security Management framework that adheres to internationally recognised standards or best practices (Core Requirement 3.2)

FIGURE 1. **PDCA cycle in Information Security Management**


Inputs
Information security requirements
Plan
Establish ISM system
Act
Maintain & improve ISM system
Do
Implement and operate ISM system
Check
Monitor & review ISM system
Outputs
Managed information security

Check; Act". PDCA underlines that information security is a practice in continuous improvement and that security threats are continuously evolving.

PDCA involves developing and implementing an information security framework and plan, applying security controls as planned, ensuring that the plan works properly, and continuously improving the plan and controls by doing more of what works and changing what does not work (see Figure 1).

AN ISM FRAMEWORK FOR TAX INFORMATION EXCHANGE

The AEOI Standard and the confidentiality assessments require tax administrations to be able to demonstrate that their practices are consistent with the ISO/IEC 27000-series standards or that an equivalent information security framework[11] is in place, and that taxpayer information obtained under an international agreement is protected under that framework.

The ISO/IEC 27000-series standards are framed broadly and do not refer specifically to tax administration. They were developed to enable any type of business organisation to implement a suitable ISM framework, as well as to demonstrate its security accreditation to other organisations.

Against this background, in the course of its AEOI confidentiality assessments, the Global Forum expert panel drew on the ISO/IEC 27000-series standards to develop a global view of data security risks to tax administrations and the best practice controls used by tax administrations around the world to mitigate those risks.

To optimise the international standards for purposes of tax administration and information exchange, the ISM requirements of CR 3.2 were organised into the six headings (SRs 3.2.1 to 3.2.6) that broadly correspond to the way in which tax administrations would normally organise their ISM arrangements using the PDCA cycle as an overarching guide.

- The overarching or "umbrella" SR 3.2.1 corresponds to the 'Plan' and 'Act' parts of PDCA. It requires that tax administrations or other authorities responsible for tax information exchanges ("relevant organisations") have an overall ISM framework comprising an ISM policy, a risk management framework, as well as a business continuity management framework.

- SR 3.2.2 to 3.2.5 correspond to the 'Do' part of PDCA:

  - SR 3.2.2 refers to security controls with respect to human resources (internal personnel and external contractors). These include that human resources are communicated their tax information confidentiality and security obligations, subjected to appropriate background checks, given appropriate training and awareness messaging, and see their

[11] Based on other international best practices such as NIST SP 800-53, CSF. Other relevant international standards that can be used within their specific scopes are the Control Objectives for Information and Related Technologies (COBIT), the Committee of Sponsoring Organisations of the Treadway Commission (COSO), the Information Technology Infrastructure Library (ITIL), etc.

  access to sensitive information terminated at the end of employment.

  - SR 3.2.3 refers to security controls to manage access to information systems (“logical access”) and premises (“physical access”) to ensure that information is accessed according to the “need to know” principle.
  - SR 3.2.4 refers to security controls to protect the IT system, including the infrastructure, networks, applications, workstations and devices.
  - SR 3.2.5 refers to security controls that protect the information or data itself, including procedures to classify data and to ensure a level of protection commensurate with its level of confidentiality classification and sensitivity (e.g. secure physical storage for information on paper, or data encryption for digital data).

- SR 3.2.6 corresponds to the ‘Check’ part of PDCA. It requires that the effective implementation of the security controls (‘Do’ parts) is monitored, the monitoring being supported by a range of logging activities covering access to and usage of physical and digital systems and data. SR 3.2.6 also requires that information is gathered from other sources, such as security incident reporting or audit activities, to inform whether security controls operate effectively in practice. Further, it requires that security controls are built into change processes, and that there is some sort of internal and external audit function.

The SRs serve as the structure for CR 3.2 in this toolkit, as outlined in Table 2:

To assist tax administrations that may already draw on the ISO/IEC 27000-series or equivalent standards, the following high-level mapping of CR 3.2 (ISM framework) to the ISO/IEC 27001 standard is provided in Figure 2.

KEY STEPS FOR THE IMPLEMENTATION OF AN ISM FRAMEWORK

As this toolkit is intended to support developing countries’ tax administrations to develop their ISM framework in line with international standards and best practices, this section presents an overview of the key, general steps for implementation of such a framework. These steps may need to be taken in multiple iterations as a developing country tax administration’s ISM approach reaches maturity.

Step 1: Scoping of the ISM framework

Jurisdictions can consider two approaches for the scope of the development of their ISM framework to participate in information exchange, depending on the maturity and complexity of their tax administration’s existing operations, IT systems, and security controls, and the modalities of EOI it participates in (e.g. automatic (reciprocal or non-reciprocal), on request, or spontaneous EOI). This is covered in SR 3.2.1.1 related to the lifecycle of information:

- Develop the ISM framework covering the full operations of the tax administration, and apply it to exchanged information, or
- Develop an ISM framework initially focussed on a secure perimeter dedicated only to its operations that handle exchanged information.

Table 2. **CR 3.2 (ISM framework) structure**

Plan, Act	SR 3.2.1 Relevant organisations should have an appropriate overall ISM system.	
Do	SR 3.2.2 Relevant organisations should have appropriate human resources controls.	SR 3.2.3 Relevant organisations should have appropriate access controls, including physical and logical access.
	SR 3.2.4 Relevant organisations should have appropriate IT system security.	SR 3.2.5 Relevant organisations should appropriately protect information.
Check	SR 3.2.6 Relevant organisations should have an appropriate operations management framework, including incident management, change management, monitoring and audit.	

Information Security Management framework that adheres to internationally recognised standards or best practices (Core Requirement 3.2)

Step 2: Defining an ISM policy

An ISM policy documents senior management's commitment to robust information security, including exchanged information. The ISM policy defines the guiding principles, and the main information security processes, procedures and controls of the tax administration. It also allocates high-level responsibilities, commits a tax administration's resources for implementation, and establishes regular reviews of the policy. The ISM policy can be improved as a result of these regular reviews to reflect the maturity of the information security approach in the tax administration.

Step 3: Identification of security risks

Implementing a sound ISM framework and policy starts with a systematic identification of the security risks to the information held by the tax administration. A risk is a scenario in which a possible threat exploits an existing vulnerability in a given asset. A clear understanding of the key assets involved in AEOI is needed, in particular, together with a critical assessment of the threats and vulnerabilities in relation to those assets.

A risk assessment should be carried out using a methodology to identify all risks arising from different threats and vulnerabilities, to assess the impact of those risks, and to determine the treatment controls to apply to those risks, i.e. the controls needed to treat the risks identified in line with their assessed impact. Information security risk management is covered in more detail in SR 3.2.1.4.

Step 4: Establishing specific policies, processes and procedures in relevant areas

Following risk identification and decision-making on the controls that will be used to treat the risks, a tax administration should reflect and document the controls it will apply in domain-specific policies, processes, and/or procedures. Box 4 provides a non-exhaustive list of examples of security policies that can be used.

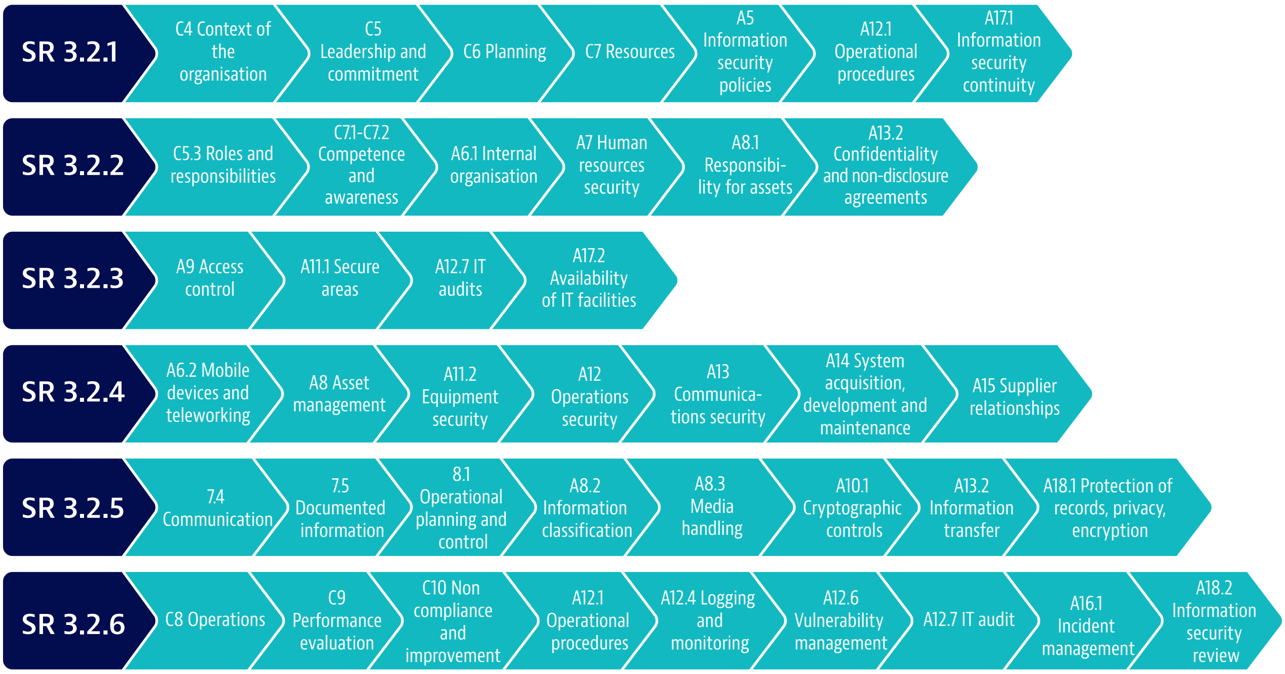
Step 5: Training of personnel

All personnel involved in ISM (and EOI) should be trained in the policies, processes, procedures and controls established to deal with security risks, to ensure their adequate implementation.

Step 6: Check the effective uptake of the ISM system

A tax administration should regularly check whether personnel are effectively implementing the ISM system, meaning the collection of domain-specific policies,

FIGURE 2. **High-level mapping of CR 3.2 (ISM framework) to the ISO/IEC 27001 standard**



SR 3.2.1: C4 Context of the organisation; C5 Leadership and commitment; C6 Planning; C7 Resources; A5 Information security policies; A12.1 Operational procedures; A17.1 Information security continuity

SR 3.2.2: C5.3 Roles and responsibilities; C7.1-C7.2 Competence and awareness; A6.1 Internal organisation; A7 Human resources security; A8.1 Responsibi-lity for assets; A13.2 Confidentiality and non-disclosure agreements

SR 3.2.3: A9 Access control; A11.1 Secure areas; A12.7 IT audits; A17.2 Availability of IT facilities

SR 3.2.4: A6.2 Mobile devices and teleworking; A8 Asset management; A11.2 Equipment security; A12 Operations security; A13 Communica-tions security; A14 System acquisition, development and maintenance; A15 Supplier relationships

SR 3.2.5: 7.4 Communication; 7.5 Documented information; 8.1 Operational planning and control; A8.2 Information classification; A8.3 Media handling; A10.1 Cryptographic controls; A13.2 Information transfer; A18.1 Protection of records, privacy, encryption

SR 3.2.6: C8 Operations; C9 Performance evaluation; C10 Non compliance and improvement; A12.1 Operational procedures; A12.4 Logging and monitoring; A12.6 Vulnerability management; A12.7 IT audit; A16.1 Incident management; A18.2 Information security review processes, procedures and security controls that implement the ISM framework (see definition in Table 3 and discussion in SR 3.2.1.3), and whether the controls are working effectively in practice.

The following sections of this toolkit provide guidance on the implementation of each of the SRs of an ISM framework (from SR 3.2.1 to SR 3.2.6) that adheres to internationally recognised standards.

SUB-REQUIREMENT 3.2.1: OVERALL ISM FRAMEWORK

SR 3.2.1 refers to tax administrations defining an overarching ISM strategy, policy and risk management framework, i.e. the organisational structures and overarching information security goals and principles that compose an ISM framework. It corresponds to the 'Plan' and 'Act' parts of PDCA and is the "umbrella" action for the implementation of the ISM system (meaning, once again, the collection of domain specific policies, procedures and controls that implement the ISM framework). An inadequate ISM framework may result in failures to effectively tackle information security risks.

SR 3.2.1 is in turn divided into five SRs:

- **SR 3.2.1.1**: Ensuring that a sound ISM framework is in place for EOI starts with the requirement that tax administrations have a clear understanding of the lifecycle of the exchanged information they hold, and be committed to safeguard its confidentiality and appropriate use.
- **SR 3.2.1.2**: Regardless of whether a tax administration is developing an ISM framework covering its full operations or the specific operations that handle exchanged information, its senior management should be fully committed to the overarching security framework. Such commitment is normally expressed in a written ISM policy.
- **SR 3.2.1.3**: A tax administration should also ensure that the ISM framework is integrated with its relevant business processes, and supported by adequate operational arrangements and ISM systems.
- **SR 3.2.1.4**: A solid ISM system should be based on the risks and threats to which the tax administration is exposed, to avoid the misapplication of scarce and valuable resources.
- **SR 3.2.1.5**: A tax administration should define and manage the risks scenarios that may disrupt the continuity of its business operations.

Box 4. Non-exhaustive list of security policies in different areas

A policy is a documented statement of a tax administration to implement processes, procedures and controls in a given domain, which can include:

- Business continuity policy (SR 3.2.1.5)
- Human resources security policy (SR 3.2.2)
- Access management policy (SR 3.2.3):
  - Physical access policy (SRs 3.2.3.1 and 3.2.3.2)
  - Logical access policy (SRs 3.2.3.3 and 3.2.3.4)
- IT security policy (SR 3.2.4.2):
  - Malware protection policy
  - Logging and monitoring policy
- Asset management policy (SR 3.2.4.3)
- Classification of information policy (SR 3.2.5)
- Clean/clear desk policy (SR 3.2.5)
- Cryptography policy (SR 3.2.5)
- Change management policy (SR 3.2.6.5)
- Incident management policy (SR 3.2.6.6)

Table 3 provides definitions of the main concepts covered in SR 3.2.1.

SR 3.2.1.1. Clear understanding the lifecycle of exchanged information and commitment to safeguard its confidentiality and appropriate use

The objective of the confidentiality assessments is to assess the suitability of tax administrations to receive specific types of taxpayer information, namely data exchanged with respect to the AEOI Standard. Therefore, SR 3.2.1 starts by setting out the expectations of tax administrations regarding the management of different types of data commonly exchanged with other tax administrations, pursuant to international exchange agreements.

Information Security Management framework that adheres to internationally recognised standards or best practices (Core Requirement 3.2)

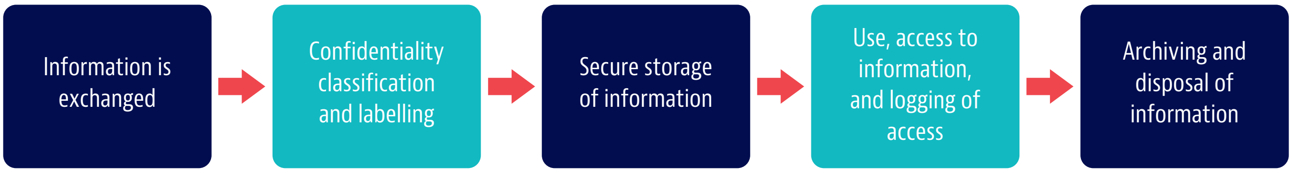
Table 3. **Glossary of main concepts**

Concept	Description
Asset	Anything of value that is involved in the realisation of processes and the generation of results. Assets can be information, people, services, equipment, systems etc.
Business continuity management	A management process to ensure the continuity of operations in the scenario of some event that disrupts normal operations.
Information security	Refers to the protection of the confidentiality, integrity and availability of information.
Information security risk	Potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation
ISM framework	An ISM framework refers to the organisational structures and overarching information security principles, aimed at guiding tax administrations to achieve ISM objectives, following a risk-based approach. The ultimate accountability for the ISM framework should sit with the most senior officials within the tax administration.
ISM policy	An ISM policy expresses the intent of the tax administration as to how it approaches information security. The ISM policy should set out the scope of the ISM system, and the general information security management objectives to which all other individual policies should adhere.
ISM system	An ISM system refers to the collection of the domain-specific policies, procedures and controls to implement the ISM framework. The ultimate accountability for the ISM system should sit with the most senior security officials within a tax administration.
Naming conventions	Refers to rules on how information is named to clearly identify it from other.
Policy	A policy is a documented statement of the tax administration to implement processes, procedures and controls in a given area. A policy answers the question "what should be done?" There should be a hierarchy of policies. For example, a policy on identification and authentication for access to IT systems will be subsidiary to an overall policy on access management. There should also be an overarching ISM policy that enumerates the overarching security principles that apply to all policies.
Practices or controls	A control or practice is a specific measure that is used to manage information security risk (i.e. mitigate or eliminate a risk). Controls can include process and procedures, as well as programs, tools, techniques, technologies and devices. Controls are sometimes also referred to as safeguards or countermeasures for an identified risk.
Procedure	A procedure is a documented set of steps and activities to implement security policies. A procedure answers the question "how should it be done and by whom?" The term procedure is often linked to the term process – processes and procedures – because a procedure is usually a more detailed representation for each step of a process. There may often be more than one procedure for each step of a process. For example, a process may concern the submission of a tax return, but there may be different ways in which submission can be executed, and therefore different procedures for each method of submission.
Process	A process is a repeatable sequence of actions with a measurable outcome. The concept of processes is critical to ISM. Measuring outcomes and acting on results is the foundation for improving processes and security. A process can be anything from a tax business process such as the submission and assessment of tax returns to the process for updating IT software. Any action that is not covered by a defined process is by definition a security risk, since there is no assurance of repeatability, and measuring and improving outcomes.
Risk mitigation	Refers to actively implementing measures to lower the impact or the probability of occurrence of a risk.
Vulnerability	Flaw in the design of an asset or its nature, or weakness arising from failure to maintain an asset.

The approach proposed in SR 3.2.1.1 is the lifecycle approach. SR 3.2.1.1 is primarily concerned with ensuring that the data held by tax administrations, including exchanged information, is protected throughout its whole lifecycle, meaning the various processes and systems for handling, storage and usage through which the data passes from the moment it is acquired by a receiving tax administration until it is disposed of (see Figure 3).

The lifecycle approach to information is also addressed in SR 3.2.5, which covers the controls required for the protection of all different types of information that the tax administration handles. However, for the purposes of the confidentiality assessments, SR 3.2.1.1 is only concerned with the category of exchanged information, which is subject to specific confidentiality controls imposed by international exchange agreements.

FIGURE 3. **Lifecycle of exchanged information**


Information is exchanged
Confidentiality classification and labelling
Secure storage of information
Use, access to information, and logging of access
Archiving and disposal of information

During each stage of the information lifecycle, tax administrations should implement specific security controls, with a clear understanding of the IT systems, departments, facilities and personnel in the different areas of the tax administration which may be involved in the lifecycle.

The selection of lifecycle controls to be implemented depends heavily on the way EOI is implemented, and the risks to EOI identified by the tax administration. Various controls are described throughout this toolkit, and tax administrations should implement them in a way that is relevant to their situation and best suits their circumstances. It is recommended that these lifecycle controls be documented, so that they are consistently implemented.

Lifecycle controls cover the following:

- The naming conventions and confidentiality classifications used to clearly identify exchanged information, not only information exchanged under the AEOI standard, but also upon request and spontaneously, as well as other relevant types of information such as Country-by-Country Reports and tax rulings exchanged under the BEPS transparency-related standards.
- The storage arrangements, meaning where and how the information is stored and the general overview of the controls used to secure it.
- The processes for the utilisation of information for authorised purposes, and to prevent unauthorised access.
- The logging arrangements to ensure that appropriate records are kept of access to the data.
- The arrangements for the archiving and disposal of information after it is no longer needed or after its retention period (if any) expires.

Table 4 provides a simplified example of an approach to the controls along the lifecycle of information exchanged with respect to the AEOI and EOIR Standards.

The default approach of the Global Forum when carrying out confidentiality assessments is that tax administrations apply the security controls used for its broader operations to exchanged information, with additional enhanced controls applied to exchanged information as appropriate.

For developing countries, however, putting in place a full ISM system across the entire operations of the tax administration may be a work in progress, and a long term and costly endeavour. Tax administrations with less overall ISM and IT maturity may therefore not be able to rely on improvements to their general security controls across the organisation in order to participate in AEOI initiatives in a timely manner under their international commitments and exchange agreements.

Developing countries' tax administrations may therefore consider prioritising the development of

Information Security Management framework that adheres to internationally recognised standards or best practices (Core Requirement 3.2)

Table 4. **Example of general lifecycle controls for information exchanged under AEOI and EOIR**

Lifecycle stage	AEOI data	EOIR data
Access and logging arrangements	Controls for access by authorised users only are established and implemented. All accesses to the AEOI database are logged and recorded.	Controls for access by authorised users only are established and implemented. All accesses to the EOIR database or to the EOIR cabinet or file room are logged and recorded.
Archiving and disposal of information	AEOI data is securely disposed of when no longer needed. If no longer needed and the retention period has not expired, AEOI data will be archived securely until the retention period expires and the data can be disposed of.	EOIR data is securely disposed of when no longer needed. If no longer needed and the retention period has not expired, EOIR data will be archived securely until the retention period expires and the data can be disposed of.
Classification and labelling	AEOI data is classified as confidential and labelled accordingly.	EOIR data is classified as confidential and labelled accordingly.
Handling and use	AEOI data is only used for tax business needs and in accordance with exchange agreements.	EOIR information is only used for tax business needs and in accordance with exchange agreements.
Storage arrangements	AEOI data is segregated from databases that hold other information.	EOIR received in digital form is segregated from databases that hold other information. EOIR in paper format is secured in locked cabinets or in file rooms accessible by authorised personnel only.

strong lifecycle controls dedicated to exchanged information, within the context of developing an ISM framework initially focussed on a 'secure perimeter' within which EOI related operations are carried out, e.g. data matching, risk analysis, case selection and audit (see Box 5).

The Global Forum can offer jurisdictions detailed guidance on implementing a secure perimeter approach upon request.

SR 3.2.1.2. ISM policy, leadership and commitment, and organisational framework

SR 3.2.1.2 requires that tax administrations manage information security through the medium of a written ISM policy that is part of an overarching security framework that clearly defines security roles and responsibilities, is owned by senior management and is kept up to date.

This SR refers to the fundamental importance of strategic leadership to have effective ISM. A crucial element is the tax administration senior managers' commitment to information security and their unequivocal support to devoting resources and funding to deliver ISM planning and implementation.

If senior managers identify information security as a priority and demonstrate their personal commitment to the success of the objectives of the ISM system, then personnel at all levels of the tax administration will generally follow the lead.

If, however, senior managers indicate that security objectives may be sacrificed, then security will be compromised. While the development of an approach for ISM is a collaborative effort organised and guided by tax business specialists, it is important that senior managers provide the overall direction.

The key elements of ISM leadership and commitment in tax administrations are:

- ISM objectives
- ISM policy
- Defined organisational roles, responsibilities and authorities for the ISM system

Box 5. **Secure perimeter for exchanged information**

What is a secure perimeter?

A secure perimeter refers to a highly secure physical and/or virtual environment within a tax administration (and therefore adequately protected in line with relevant standards), that would enable jurisdictions to receive, keep safe, and handle information exchanged automatically, spontaneously or on request whilst longer term efforts are made to implement international ISM standards across the whole tax administration. It is a tactical approach that may be implemented at a lesser cost, and within a shorter timeframe, than if the necessary security controls are implemented across the entire operations.

A secure perimeter involves tax administrations managing and exercising control over the lifecycle of exchanged information by maintaining a high degree of separation between it and the other processes, technology, personnel and data sets already used for the broader domestic tax administration. It would generally involve a secure organisational unit within the administration, where tighter security controls can be put in place to meet the strict demands of exchange agreements, exchange partners and the Global Forum standards (e.g. an office within a central headquarters building, or a building in itself).

In practice this means the tax administration would handle and use data sets received from exchange partners solely within the secure perimeter. Technological, physical and human resources would need to be allocated to process exchanged information within the perimeter, as well as to conduct data matching, compliance risk assessments, reviews, audits or other compliance activities within the confines of the perimeter.

How can a secure perimeter be implemented?

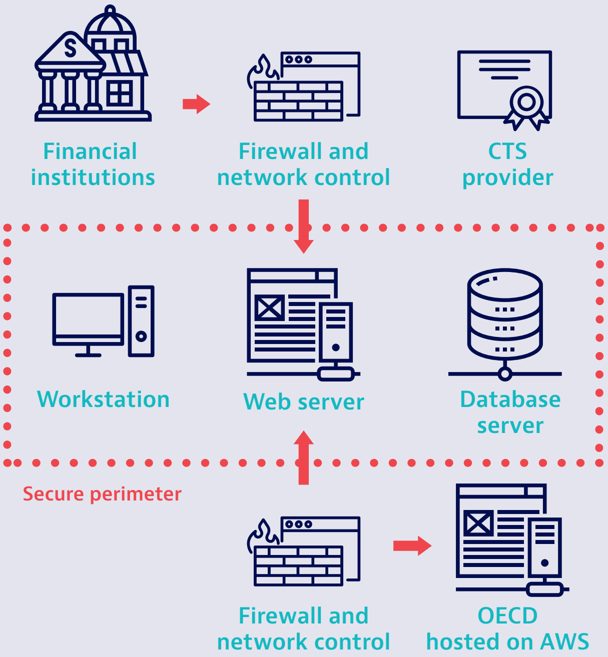
In deciding how to implement a secure perimeter, a tax administration should first look closely at how it might best fit with existing operational structures. For example, if a tax administration already has a relatively more secure internal organisational unit for handling particularly sensitive operations (e.g. a high wealth individuals unit or a more secure building in the capital city), it could be possible to incorporate the handling and use of exchanged information within that existing unit.

Another approach might be to look at how the work with exchanged information maps to existing operations. For example, if there is a single organisational unit that handles large taxpayers and wealthy individuals, it may make sense to integrate the secure perimeter within that existing unit as these are the taxpayers most likely to be the subjects of information received from exchange partners.

Key implementation components might generally include:

- Installation of one or more dedicated computers to access information received under EOI.
- Special security controls for physical access to the location, e.g. turnstiles activated by cards, closed-circuit TV (CCTV) for the area, only one person can enter at a time, alarms, etc.
- Appropriate training and awareness for the personnel, e.g. tax compliance officers, who will be working within the secure perimeter making use of exchanged information.
- Setup of an overarching ISM governance structure, policy and processes applicable to the secure perimeter that are sponsored by the senior management of the tax administration.
- Acquisition, production and delivery of minimum IT controls for the system(s) used to process and utilise exchanged information, including: system design document and controls plan, gateway controls, internal network segmentation, whitelisting, access management and authentication, limiting staff and computer access, centralised audit logging, change management, communication encryption, risk management and vulnerability scanning.

The following is an example of a secure perimeter network architecture for illustrative purposes only.



Information Security Management framework that adheres to internationally recognised standards or best practices (Core Requirement 3.2)

ISM objectives

Tax administrations should define clear objectives for the ISM system and for what is expected to be achieved. Depending on the maturity or scale of the tax administration, the planning and objective setting can be carried out at various levels. ISM objectives can be defined as part of the strategic planning of the tax administration, as part of the IT strategy or, ideally, as part of a dedicated information security strategy.

Regardless of how ISM objectives are defined, they should be supported with committed resources and funding for their achievement and with clearly defined responsibilities for the individual objectives and activities.

The key ISM objectives in any tax administration should be to:

- Protect sensitive taxpayer information held and other relevant information assets, consistent with domestic confidentiality and data protection laws and confidentiality commitments under international treaties.
- Mitigate the security risks to information through security controls and access measures proportionate to those risks, while at the same time enabling users (personnel) to access the information they need to carry out their work effectively.
- Establish the reporting of security incidents by personnel and encourage an open and positive work environment in which personnel are willing to acknowledge error and strive collectively to improve information security on a continuous basis (PDCA).
- Establish reporting arrangements and effective measurement and review tools (with accurate and secure data) to check whether the objectives are being achieved and whether the security controls that support them are working in practice.

ISM policy

The way in which ISM objectives are communicated to tax administration personnel is first and foremost through an overarching ISM policy.

Tax administrations usually have various specific policies for different domains, e.g. for managing human resources, physical access to premises and logical access to IT systems, the use of IT equipment, vulnerabilities, etc. These specific policies will usually be managed by different operational areas within the tax administration, which could lead to a risk of inconsistency across policies.

Box 6. **Example of ISM policy general structure**

An ISM policy can have varying levels of detail, but in general it may have the following structure:

- Statement of purpose – why the ISM policy exists.
- Description of the intended audience – who should read it and to whom it applies. This can be both internal and external parties, e.g. tax administration personnel and IT service providers.
- Organisation's approach to ISM objectives and principles – i.e. protection of the confidentiality and integrity of the information while ensuring its availability for personnel to fulfil their functions.
- High level overview of the key areas and security principles, with general references to specific policies. Although an ISM policy sets the overarching framework for information security, the policy should at minimum address the approach for the following areas:
  - IT security.
  - Physical security.
  - Human resources security.
  - Business continuity management.
- Key roles and responsibilities, with reporting, escalation and measurement arrangements.
- Authority for review – who approves and reviews the ISM policy, and how regularly.

It is therefore good practice to establish an overarching ISM policy that expresses the intent of the tax administration as to how it approaches information security. The ISM policy should set out the scope of the ISM system, and the general information security management objectives (as outlined in the previous heading) to which all other individual policies should adhere.

The ISM policy should also reflect the commitment from senior management to provide the necessary resources for the implementation of its security objectives. An example of the general structure of an ISM policy is provided in Box 6.

Tax administration senior managers should ensure that personnel (including external contractors) are aware of the ISM policy and its contents, so a comprehensive communication and training programme is recommended. Security training and awareness is addressed in more detail in SR 3.2.2, related to human resources controls.

ISM key roles and responsibilities

Tax administrations' senior management, through the ISM policy, should allocate clear responsibilities for ISM to all personnel within the scope of the ISM policy, and to at least the following groups or persons:

- Key responsible person for information security.
- Senior management of the areas covered by the ISM policy.
- Head of the IT department.
- IT department personnel.
- Internal audit.

The key responsible person for information security is commonly known as the Information Security Officer (ISO), but depending on the organisational structure and culture of the tax administration, they may have a different designation.

It is generally advisable that the ISO has a direct reporting line to senior managers of the tax administration, and that the ISO is not from within the IT department. This is because the ISO should be responsible for controls and policies in a number of security domains, across processes that do not fall only within the scope of IT (physical security, human resources, internal audit, etc.). Box 7 provides an outline of the desired capabilities and roles of an ISO.

A clear delineation of roles and responsibilities as between the IT personnel and the information security personnel is desirable. Also, clear communication lines between them should be defined and established.

Box 7. Capabilities and roles of an Information Security Officer

What qualifications and experience should the person have?

An ISO should have a mix of technical and organisational skills, a clear understanding of the information security subject and experience in a number of security domains. The ISO should be comfortable with discussion of technical issues, and understand the business, regulatory and statutory requirements for security.

The specific qualifications of an ISO may depend on the scale of the tax administration's operations, but the single most important requirement is their belief in the importance of appropriate security and of communicating it to others.

For smaller tax administrations, an ISO may be one person from the tax administration with strong security and IT competences. Larger tax administrations may require teams of multiple specialists covering each area of the business, and in such situations an ISO may require a skillset that is often not available internally in the tax administration.

Where should the ISO sit within the organisational structure? How should the ISO be managed?

The ISO, as the principal security officer, should have direct access to the head of the tax administration. The ISO's functions can be outlined in Terms of Reference or a job description approved by the head of the tax administration and that set out, among others, the key security deliverables, what sort of reports the ISO would be expected to provide, how often, etc.

Depending on the size of the tax administration, an ISO might have a team that provides support for the implementation of the responsibilities and activities in scope.

The focus of IT personnel should be the effective implementation and operation of the IT systems and the integration of security aspects in their development, as defined in the policies. Tax administrations should clearly document the hierarchical and reporting lines as between IT and security personnel in an organisational chart.

Information Security Management framework that adheres to internationally recognised standards or best practices (Core Requirement 3.2)

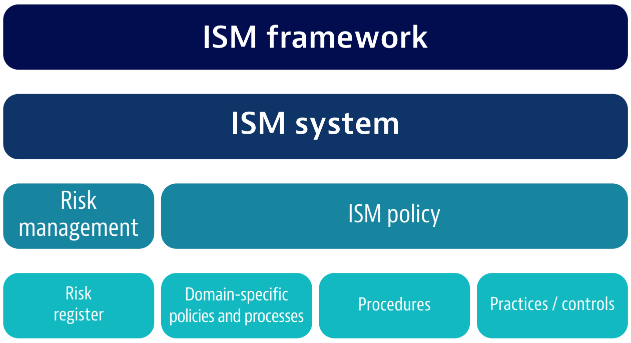
SR 3.2.1.3. ISM system

SR 3.2.1.3 requires tax administrations to address information security through appropriate operational arrangements and as an integrated part of the management of relevant business processes. In short, this means having an ISM system integrated with business operations.

As defined in Table 3, the ISM framework refers to the organisational structures and overarching information security principles aimed at guiding tax administrations to achieve ISM objectives, whereas the ISM system comprises the domain-specific policies, procedures and controls that are required to implement the ISM framework.

The size of a tax administration, the complexity of operations and the maturity of its IT systems all influence the level of detail of an ISM system (see Figure 4).

FIGURE 4. **Components of the ISM framework and ISM system**



The components of an ISM system should be developed based on the risk management assessments carried out by the tax administration. Risk management is discussed in detail in SR 3.2.1.4.

An ISM system can be represented though a high-level document (such as a manual) that comprises the different sets of policies, procedures and controls related to a particular security domain. Tax administrations can consider the following structure for their ISM system document:

- Introduction.
- Scope of the ISM system.
- Organisational chart, roles and responsibilities, and reporting arrangements between stakeholders.
- ISM policy.
- Main ISM processes.
- Risk management approach, and the risks identified.

Box 8. **Example of a policy in a specific security domain within the context of an ISM framework and system**

ISM framework. Objective: Protect sensitive taxpayer information and other relevant information assets.

ISM system and policy. Policy for the protection of AEOI data held by the tax administration, consistent with the risk assessment carried out on that information asset. All access to AEOI systems and databases is strictly controlled through the use of complex passwords.

Implementation of password policy, as a control. In Active Directory, the group policy for the system where AEOI information is stored is set to: Passwords must have at least 15 characters and must be changed every 180 days. Passwords cannot be repeated for the last 10 iterations, and they must not be shared in any shape or form. Personnel is instructed on the use of passwords.

Implementation of password policy, as a procedure. The ISO is responsible for ensuring that the password policy is applied and enforced in all AEOI systems and databases. The ISO should be consulted when systems are built to ensure the policy is correctly applied. The ISO should coordinate with the IT specialists (usually system administrators) to ensure that the policy is being implemented and that it is working effectively. If the policy is not being adequately implemented, then remedial measures should be taken (improved guidance to personnel, etc.). The ISO should also carry out spot checks regularly, to ensure that personnel understand the policy and apply it correctly. The ISO should actively engage with those working in security operations to establish whether operational controls such as logging, monitoring, and incident management are identifying issues or failures with the implementation of the password policy.

- Various policies in a particular security domain to deal with the identified risks (with reference to specific procedures or controls). There are various general domains of information security, and for the purposes of the confidentiality assessments, the following should be addressed by tax administrations in their ISM system:
    - Human resources (SR. 3.2.2)
    - Access management (SR 3.2.3)
    - IT security (SR 3.2.4)
    - Protection of information (SR 3.2.5), and
    - Operations management (SR 3.2.6).
- Approach to the control of the documented policies of the ISM system.
- Approach to internal audit of the ISM system.
- Periodicity of review of the ISM system.

Box 8 provides a simplified example of how a policy in a specific security domain might be organised within the context of an ISM framework and system.

SR 3.2.1.4. Information security risk management

Human and financial resources in a tax administration are limited, so it is good practice to design an ISM system based on an assessment of the security risks to which the tax administration is exposed, so that the limited resources are efficiently allocated.

SR 3.2.1.4 requires that tax administrations systematically manage their information security risks, taking account of the threats, vulnerabilities, and impacts.

Under international standards for risk management such as ISO31000 and ISO27005[12], information security risks can be defined as the "potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation”.

Tax administrations are expected to have a solid and comprehensive risk management process, reflected in a risk management methodology. This methodology should outline the steps of the risk management process, the specific responsibilities in each of the steps and the criteria used for assessment of risks.

Tax administrations can have a specific risk management methodology only for the ISM system, or can use a methodology used for other areas of the tax administration, and apply it to the ISM system. If the latter approach is used, it is important to adjust the criteria to information security.

In general, the methodology for information security risk management includes the steps outlined in Table 5. Its details are, however, for reference only and tax administrations are encouraged to use the methodologies that best adapt to their own organisations.

Risk management is a continuous process, and risks should be reviewed and assessed at regular intervals. Importantly, the effectiveness of risk-mitigation controls should be periodically monitored. In the case of a risk scenario, tax administrations should initiate the procedure for incident management, described in detail under SR 3.2.6.6.

It is crucial that tax administration personnel are aware of the key information security risks, and that these are communicated as part of awareness programmes or other training activities carried out by the tax administration.

Tax administrations can document the outputs of the risk assessment exercise in a risk register or any other tools used by them to support their risk assessment activities. A sample risk register, with reference examples for the asset groups “human resources” and “information assets” and based on the methodology outlined in Table 5, is presented in Table 6.

This risk register is for illustrative purposes only. Tax administrations may consider separate risk registers for different asset groups, for IT and non-IT domains, or use a centralised register. They are encouraged to use the approach that best adapts to their own organisation.

[12] www.iso.org/iso-31000-risk-management.html and www.iso.org/standard/75281.html

Information Security Management framework that adheres to internationally recognised standards or best practices (Core Requirement 3.2)

Table 5. **Sample risk management methodology based on the ISO27000-series guidance**

Step	Description	Output
1.Asset identification	Prepare an asset inventory of major assets of the organisation, with the asset owner identified. An asset owner is the person responsible for the management and use of the asset. Assets can vary depending on the scope of the assessment. For instance, for an overarching risk assessment for AEOI, only business processes and systems related to AEOI might be identified as assets. For a risk assessment only related to IT systems, the specific components of IT systems (hardware, software) would be identified as assets.	**Asset categories can include:** • Business processes • Human resources • Information assets • Image and reputation • Software assets • Hardware assets • Other physical assets • Outsourced services • Internal supporting services
2.Asset valuation	Conduct a valuation of assets in relation to their importance for the tax administration and for achieving its information security objectives.	**Possible asset values:** **1.** Very little importance **2.** Little importance **3.** Medium importance **4.** Big importance **5.** Very big importance
3.Identification of risk scenarios	This step can be divided into: • Identification of asset threats and vulnerabilities, or risk scenarios. • Assessment of the likelihood of the risk scenario occurring.	**Possible likelihoods for risk scenarios:** **1.** Rare chance of happening **2.** Unlikely to happen **3.** Moderate possibility of happening **4.** Likely to happen **5.** Almost certain it will happen
4.Impact assessment	Assess the impact over the confidentiality, integrity and availability of information and/or over the security objectives, if the risk scenario occurs.	**Proposed impact values:** **0.** No impact **1.** Little impact **2.** Medium impact **3.** Big impact
5.Risk valuation	Conduct risk valuation. A simple formula can be used that takes into consideration the value of the asset, the likelihood of the risk scenario and the impact value.	**Formula for risk valuation:** asset value * likelihood of risk scenario * impact value
6.Definition of level of acceptable risk	Define the level of acceptable risk, based on the importance of the assets, domestic regulatory requirements or on obligations arising from treaties. An acceptable risk can be defined as a risk for which the management of the tax administration is willing to accept the consequences of occurrence. Usually for such risks, the cost of implementing a mitigating control outweighs the benefits of implementing that control. However, even if a risk is defined as "acceptable", that risk should always be monitored, as risk can change and evolve. Upon change in business requirements or availability of resources, the decision for acceptable risks can be modified.	The decision should be documented and revisited at regular intervals.
7. Risk treatment	Identify the suitable risk treatment controls.	**Asset categories can include:** • Risk acceptance: no specific control is taken, e.g. no encryption is applied to certain data while at rest. The risk is, however, monitored. • Risk mitigation: controls to reduce the likelihood of the risk happening, e.g. use of firewalls and encryption to protect a database. • Risk avoidance: the impacted service or application will be completely disabled, reducing the likelihood to zero, e.g. the system will not be connected to the internet to prevent hacker attacks. • Risk transfer: the specific risk will be managed by another entity (i.e. cyber insurance for data breaches). This option is recommended only for mitigation of the financial impact of a risk and should be used in very limited cases.
8.Risk monitoring and reassessment	Based on the regular monitoring of the implementation of controls, internal audit and other review processes, update the risk management process and its results.	Recommended interval for review is one year or at major change of environment.

Table 6. **Sample risk register structure**

Asset group	Asset	Asset value (1-5)	Threat	Vulnerability	Likelihood of occurrence (1-5)	Impact value (0-3)	Risk valuation (asset value* likelihood* impact	Selected controls if treatment is needed
Human resources	Head of tax administration	4	Unavailability for key decision making	Constant change of authorities	4	3	48	Mitigate: Delegation of authority.
	Key IT staff	5	System administrator is unavailable for emergency patch implementation	Only one system administrator in the IT department	3	3	45	Mitigate: Establish a team of 3 system administrators.
Information assets	Domestic taxpayer data and AEOI data (digital format)	5	Data breach and disclosure of confidential information	System vulnerabilities	3	5	75	Mitigate: Penetration testing, data is encrypted when in transit, firewall controls, backup of data, all accesses to the database are logged and recorded, access on a need-to-know basis.
	EOI information held in paper format	5	Unauthorised person accesses the file room and discloses confidential information	File room is not adequately secured	3	5	75	Mitigate: File room can only be accessed by authorised personnel, using an access code. All accesses to the file room are logged and recorded.

SR 3.2.1.5. Business Continuity Management

SR 3.2.1.5 requires that tax administrations have appropriate arrangements to manage and maintain business continuity. This refers to how a tax administration ensures it can continue carrying out its main business processes, including tax collection and AEOI, in the scenario of some event that disrupts normal operations. Such event can be a natural disaster, a pandemic, a ransomware attack or a technical incident that leaves the IT systems not operational.

Business continuity and the related planning (Business Continuity Plan – BCP) are closely linked to the risk management process. Business continuity is a management process that includes the identification of risk scenarios, the assessment of their impact, the definition of a BCP to ensure the continuity of operations in case a risk scenario occurs, and the testing and review of the BCP as well as training of personnel on the BCP, as shown in Figure 5. The common steps for BCP are outlined below.

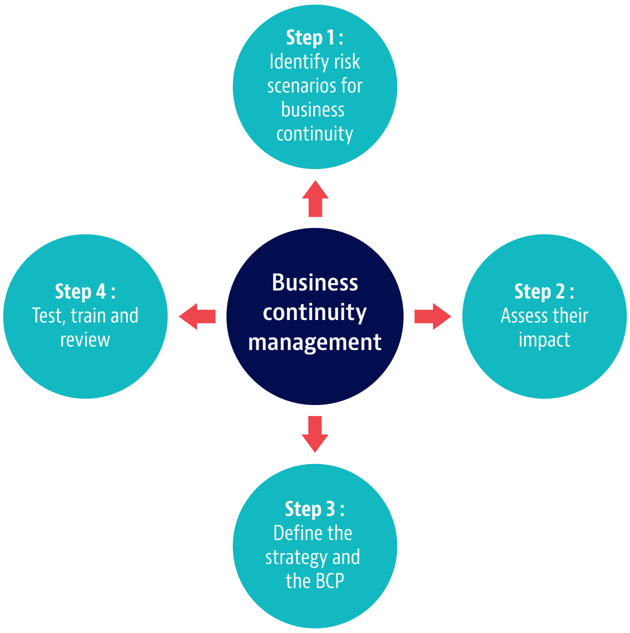
Step 1: Identification of risk scenarios for business continuity

Senior managers and key representatives from the areas involved (IT department, physical security department, human resources department, etc.), jointly identify the probable risk scenarios that could disrupt operations in the tax administration. Risk scenarios can include natural disasters, pandemics or technical catastrophes which may cause a combination of:

- Unavailability of personnel.

- Unavailability of physical facilities.
- Unavailability of information and communications technology systems.

FIGURE 5. **Business Continuity Management process**


Step 1 :
Identify risk scenarios for business continuity
Business continuity management
Step 4 :
Test, train and review
Step 2 :
Assess their impact
Step 3 :
Define the strategy and the BCP

Step 2: Assessment of the impact of risk scenarios on operations

Tax administrations should assess and document the potential impact of each risk scenario on the continuity of operations, e.g. how a specific risk scenario would impact AEOI operations or tax collection processes. The impact can be expressed in qualitative terms (such as a tax administration not being able to exchange information on time) or quantitative terms (such as the amount of taxes not collected on time).

Step 3: Definition of the strategy and the BCP

Tax administrations should define a strategy to respond to and overcome the impact on operations if a risk scenario materialises. Each BCP should cover three main stages (see Box 9 for an example of a BCP structure):

- Immediate response, giving priority to personnel safety if applicable.
- Enabling core functionalities to be restored. For this purpose, a BCP should identify the:
    - Key systems and their priority for restoration.
    - Critical key personnel or suppliers involved and their personal contact details (email, private phone).
    - Critical information, paper documents and/or backups or external drives that need to be taken to a back-up location.
    - Person who makes the decision to return to normal operations.
- Procedure and steps for return to normal operations.

Box 9. **Example of a BCP structure**

1. Recovery priorities. Essential business operations that have priority for recovery and have to be relocated to an alternate location.
2. Relocation strategy and alternative location. The alternate business site is to be used in the event of a disaster or disruption that inhibits the continuation of business processes at the original tax administration site. This strategy could include both short-term and long-term relocation sites, depending on the severity of the disruption.
3. Backup of critical digital and paper information.
4. Recovery stages:
    - **a.** Disaster occurrence.
    - **b.** BCP activation.
    - **c.** Relocation to alternate location.
    - **d.** Recovery, i.e. specific activities or tasks to recover normal and critical business operations.
    - **e.** Return to normal operations.
5. Restoration plan, i.e. disaster recovery and IT teams to maintain, control, and periodically check all the records that are vital to the continuation of business operations and that would be affected by facility disruptions or disasters. These teams periodically back up and store the most critical files at an offsite location.
6. Recovery team. Roles and responsibilities. Contact details.

Box 10. **Example of a BCP in a tax administration**

The BCP of Jurisdiction A's tax administration includes detailed steps to ensure the tax administration is able to recover from a major disruption of business operations. The BCP has been prepared taking into consideration major risk scenarios, although the plan is general enough to be applied to most threats.

The BCP details all stakeholders that need to be involved in case of an emergency that disrupts operations, and their contact details are updated immediately if there is a change so they can be contacted promptly.

The BCP lists all critical IT systems and their priority for recovery. The BCP sets out that all critical IT systems should be recovered within 24-48 hours, and the return to normal operations should not exceed a week. The tax administration has an alternate processing site in case operations need to be relocated.

Personnel is trained yearly in relation to the BCP, and the BPC is published in the intranet of the tax administration.

The tax administration conducts desktop simulations of the BCP twice a year, and drills at least once a year. The simulations aim to assess the readiness and knowledge of personnel regarding the BCP, to gain assurance that all personnel know the roles they need to assume in case of an emergency, and the identification of possible gaps in the BCP. The BCP is improved following these simulations.

BCPs should be revised regularly for changes in risk scenarios, updating key personnel and contact information, changes in the type of information held or in the IT system, etc.

Step 4: Testing, training and review of the BCP

BCPs should be tested at least annually, with full rehearsals or drills. The main objective of a test is to verify that personnel know what to do during an emergency, as defined in the BCP. The findings of BCP tests should be reported and used to further improve the BCP.

It is of the highest importance that personnel are given training on BCP. Regular awareness sessions should be carried out for all personnel involved. See Box 10 for an example of BCP testing and training.

Managing scenarios of unavailability of information and communication technology systems usually falls within the responsibility of the IT department. This point is addressed in more detail in SR 3.2.4.5, related to the continuity of IT services based on Service Level Agreements.

SUB-REQUIREMENT 3.2.2: HUMAN RESOURCES CONTROLS

Human resources controls refer to the legal and administrative policies and procedures in place to manage the human resources of tax administrations (generally, personnel and contractors) with a focus on ensuring that they respect and protect the confidentiality of tax information.

Personnel have access to sensitive information about the affairs of taxpayers, as well as the policy and conduct of tax administration, e.g. in the course of tax audit, risk analysis and investigative processes. Personnel are also closely associated with every stage of the lifecycle of exchanged information.

Therefore, tax administrations should put in place controls along the lifecycle of employment to ensure that personnel, as well as third party or external contractors, can be trusted to ensure confidentiality. Trust between an employer and its personnel is based on initial screening during recruitment (often followed by initial trialling via probation), and years of the employer-employee relationship.

This section is divided into four headings: a brief outline of the employment lifecycle; then, the activities and processes at each of the three main lifecycle stages: recruitment, employment, and termination.

The three lifecycle stages are described in detail, including the specific controls that may be applied. Table 7 provides definitions of the main concepts covered in SR 3.2.2.

Information Security Management framework that adheres to internationally recognised standards or best practices (Core Requirement 3.2)

Table 7. **Glossary of main concepts**

Concept	Description
Awareness	Awareness is about employees being regularly exposed to security messages alerting them of IT threats/risks or other security threats/risks, usually communicated to all employees at the same time, whether that be personnel in a particular work area or across the whole breadth of the tax administration, even including external third parties, etc.
Non-disclosure agreement	Formal statements or contracts defining the rules for the non-disclosure of confidential information to third parties.
Phishing	Type of online scam where criminals send out fraudulent email messages that appear to come from a legitimate source and trick the recipient into sending confidential information, such as credentials for access to systems.
Social engineering	Refers to maliciously exploiting the trusting nature of personnel in order to obtain information that can be used for personal gain. This activity is also known as "people hacking".
Training	Training is about tax administration personnel (employees and contractors) acquiring and developing the knowledge, skills and core competences needed to integrate confidentiality and security into tax processes.

Personnel lifecycle

SR 3.2.2, reflecting international standards, requires tax administrations to have in place various policies and procedures (i.e. the controls) across the three stages of the employment lifecycle: controls that relate to recruitment (SRs 3.2.2.1 and 3.2.2.2), controls that relate to the ongoing employer-employee relationship (SRs 3.2.2.3 and 3.2.2.4), and controls that relate to the termination of the employment (SRs 3.2.2.5). The key controls are highlighted in Figure 6.

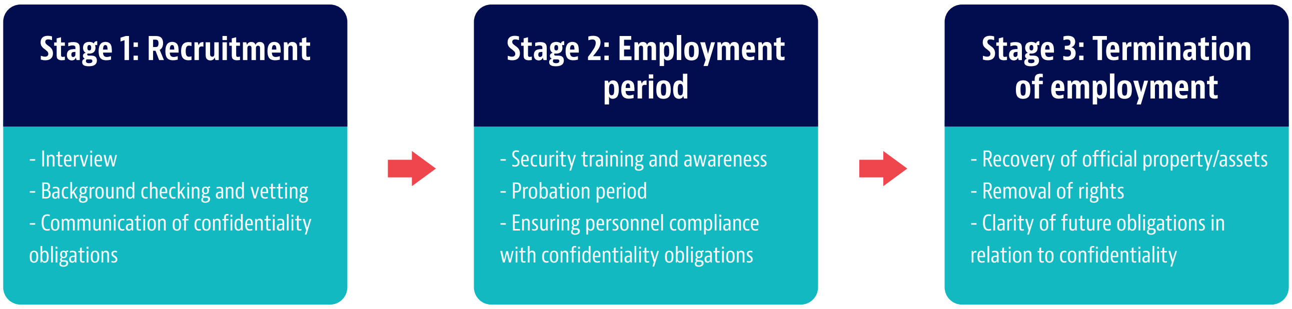
Types of personnel in a tax administration

Controls along the employment lifecycle should apply to all personnel (which in a broad sense includes employees, both permanent and temporary, and external service providers and contractors). Tax administration personnel are not a single class of employee and it is not uncommon to find the categories mentioned in Table 8:

There may be other categories to consider, depending on the particular context of the jurisdiction and its labour laws.

Tax administrations should take into consideration all their different categories of personnel when assessing the various types of processes that apply to them throughout the lifecycle of their employment. For example, they should establish suitable controls in respect of external third parties who are hired to perform sensitive functions (e.g. administering the systems that contain exchanged information) and deliver role-tailored training on the protection of the confidentiality to all personnel who administer or handle sensitive taxpayer information, regardless of the contract modality.

FIGURE 6. **Employment lifecycle and controls to ensure confidentiality**



Stage 1: Recruitment

- Interview
- Background checking and vetting
- Communication of confidentiality obligations

Stage 2: Employment period

- Security training and awareness
- Probation period
- Ensuring personnel compliance with confidentiality obligations

Stage 3: Termination of employment

- Recovery of official property/assets
- Removal of rights
- Clarity of future obligations in relation to confidentiality

Table 8. **Types of personnel in a tax administration**

Type	Description
Employee	Usually persons hired on the basis of an open ended or time-bound but renewable contract.
Temporary staff	Usually persons hired on the basis of a time-bound contract for a specific purpose (e.g. consultancy services).
Civil servant	Persons appointed to tenure in public administration, commonly a lifetime position.
External contractors	In this case, there can be two types of contractual relationships: ● External contractors hired to provide a specific service, such as to provide an IT software system, or to clean the premises. ● Contractors taken on to fulfil a particular role, such as a short-term role, or a role for which there are no suitably qualified employees. For example, an expert hired to provide a two-week in situ training to personnel on the use of a specialised system.

Specific security controls directly applied to third party contractors are covered in more detail in SR 3.2.4.4 about the management of supplier service delivery.

The controls applied may also depend on how the human resources function of the tax administration is organised. Human resources is not a tax administration function per se but rather a generic function on which the tax administration relies. As such, human resources is not always managed within the tax administration, e.g. some jurisdictions may have a single human resources department for the entire Ministry of Finance or for the entire public sector, or manage certain personnel centrally (such as the cadre of civil servants); whereas others without civil servant status are managed within the tax administration.

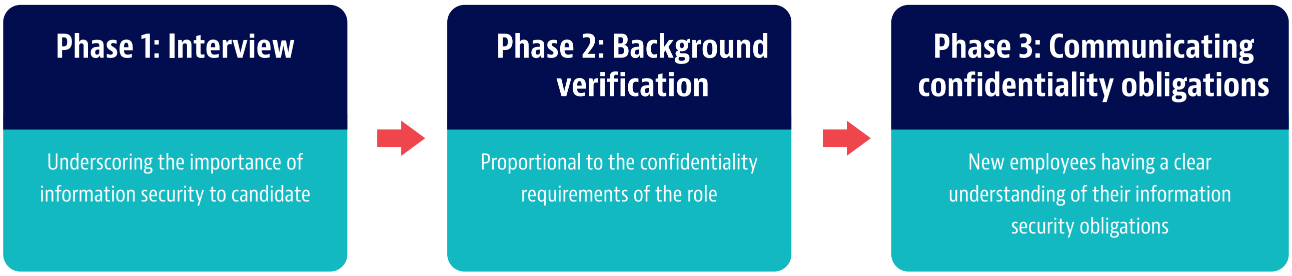
Whichever the organisational structure in place, jurisdictions should be able to correctly identify the place of the human resource management function in their overall scheme of government and its linkage with the tax administration. This allows them to self-assess what different governmental agencies or departments involved should be doing to ensure that controls commensurate with the sensitivity of the tax administration function are in place in the different policies and procedures.

The following sections provide guidance on common controls to apply in respect of the three stages of employment.

SRs 3.2.2.1 and 3.2.2.2. Stage 1: Recruitment controls

This section is about security controls during the recruitment process. These controls refer to the checks and arrangements in place to ensure that prospective personnel can be entrusted to handle confidential information. Controls should be consistent with the relevant laws and regulations of the jurisdiction (e.g. tax code, civil service regulations), and proportional to the business requirements, the classification and sensitivity of the information to be accessed, and the perceived risks.

FIGURE 7. **The recruitment process**


Phase 1: Interview
Underscoring the importance of information security to candidate
Phase 2: Background verification
Proportional to the confidentiality requirements of the role
Phase 3: Communicating confidentiality obligations
New employees having a clear understanding of their information security obligations

Information Security Management framework that adheres to internationally recognised standards or best practices (Core Requirement 3.2)

First, SR 3.2.2.1 requires that tax administrations ensure that security roles and responsibilities of employees and contractors are defined, documented, and clearly communicated in terms of engagement, and regularly reviewed in accordance with the ISM policy (this should include confidentiality and non disclosure agreements). This is discussed further below.

Second, SR 3.2.2.2 requires that tax administrations undertake background checks with appropriate vetting of all candidates for employment, employees and contrators, in accordance with accepted best practices and perceived risks. This relates to the recruitment process, which can be segmented into three phases, each with its own set of controls related to confidentiality (see Figure 7).

Phase 1: Interview

The interview process should underscore the importance of confidentiality and good information security to potential candidates. For example, the recruitment form may have an appropriate security classification marking, with an indication to prospective personnel as to the level of confidentiality that the role will entail. In addition, candidates shortlisted for an interview may

Table 9. **Types of background verifications during the recruitment processn**

Background check	Description
Checks of the evidence for candidates' submissions	This entails checking the professional experience, educational and technical qualifications, references, etc. submitted by candidates. A candidate submitting false information would fail the standards of probity that a job with a tax administration requires. However, it may not be necessary to carry out checks on all the qualifications and references submitted. Sample checks based on some risk-based agreed criteria or complete checks for all candidates in some areas may suffice to ensure that applicants' submissions are acceptable.
Criminal record checks	A criminal records check is usually required alongside application information. In some jurisdictions, having a criminal record is considered wholly inconsistent with employment in tax administration. If a criminal record is no bar for a tax administration when recruiting personnel, it might be necessary that it applies certain limiting criteria. These may include the seriousness of the offence, the time elapsed since the offence was committed, etc. In addition, tax administrations may take compensatory measures if a candidate with a criminal record is hired, e.g. the establishment of probationary or induction periods (with an exit criteria) during which the individual would be under enhanced supervision. In relation to criminal acts committed during employment, jurisdictions should make it clear to prospective personnel that any criminal charges have to be reported and may have consequences (such as termination).
Financial record checks	Another type of check can be financial record disclosure, in particular for people in senior positions. Although this may be a check relevant to tax administration work, its application may depend on the particular context of the jurisdiction, e.g. if corruption is perceived as a particular issue. In some jurisdictions, it may be carried out as part of a wider review of the affairs of those seeking clearance to work with the most sensitive information (see vetting immediately below).
Vetting	Some jurisdictions have department-specific or cross-government vetting or clearance services (often integrated with the national security services), which carry out different types of suitability checks to get a good understanding of an individual's background and character. These checks are usually required before individuals commence a job involving access to classified information, and may vary depending on the level of classification (e.g. protected, secret, top secret). It is common for certain tax administration personnel to handle data classified at high levels, e.g. financial and commercial records of large taxpayers or of persons in political office. This multi-level vetting supports government agencies and their personnel working with information at different levels of security. Vetting may include: proof of identity, criminal convictions and misdemeanours, failed drug-testing, credit rating, bankruptcy, income for the last 5 years, gambling issues, etc. For advanced vetting, the list can include interviewing the personnel, as well as a sample of other family members, friends and associates.

be explained their confidentiality obligations and the consequences of a breach (administrative, criminal), should they be awarded the position.

Phase 2: Background checking and verification

This refers to the application of background checks, vetting, and other appropriate verification arrangements to all candidates for employment, including permanent and temporary employees, contractors, etc. Background checks can have different levels of scrutiny, and are usually proportional to the type of role and its confidentiality requirements (see Table 9).

Although these checks and verifications are presented as applicable to the commencement of employment, it is also important that they are refreshed periodically, and some of them may need to be replicated in the course of employment under certain circumstances. For example, when there is a significant change in the personnel's role or they move to a more sensitive role, with access to information that is more sensitive or of a higher classification. Vetting, in particular where the vetting clearance is above the basic level, should normally be time-bound, with a process for vetting levels to be reviewed and clearances updated.

In the case of external contractors, tax administrations should also carry out background checks and verifications. However, tax administrations may decide to outsource them to the contractor itself. The contractor would undertake to check its own personnel and to ensure that they all comply with the tax administration's security policies. In such a case, the tax administration should ensure that the third party appropriately carries out the background checks and fulfils the terms of its contract. Controls for third party contractors are also covered in SR 3.2.4.4, about supplier service delivery management. In the case of long term contractors, tax administrations may require the contractor or its personnel's background verification to be refreshed from time to time (e.g. in line with minimum intervals established by law or by general personnel policy). Box 11 provides some examples of recruitment controls.

Box 11. **Example of recruitment controls**

Jurisdiction A's tax administration performs background verification checks in relation to all personnel. During the recruitment process, a certificate from the Ministry of Interior is obtained to confirm that no criminal sanctions have been imposed and that the person is not undergoing criminal proceedings. Also, proof of a candidate's educational qualifications is requested. Previous employers are contacted.

Where the person is to access classified information, such as EOI information, controls also include a vetting and security clearance process with inquiries into the person's financial affairs, nationality, mental health and other relevant personal information. If the person has already been employed with the tax administration, factors such as proper conduct in dealing with information and documents and conduct in general during their time of service are taken into account.

If the tax administration needs to engage contractors to handle EOI information, or to obtain software, hardware or services, the personnel of such contractors would also be subject to the background checks, vetting and security clearance as for regular personnel, depending on the perceived risks and the type of service to be provided. The company itself would also be reviewed to check for any reputational issues.

Phase 3: Communicating confidentiality roles and obligations upon recruitment

As described in SR 3.2.2.1, new personnel should be given a clear picture of their obligations as part of recruitment, commencement and employment. Confidentiality and information security roles and responsibilities should be clearly documented and communicated to all recruits and personnel, for instance via:

- Tax secrecy provisions in relevant legislation, e.g. Tax Code, Civil Service Code.
- The ISM policy or other ISM documents.
- Contracts, terms and conditions of employment, or other official appointment instruments signed by personnel.
- Confidentiality and non-disclosure agreements or statements, e.g. inclusion of a confidentiality clause in contracts for personnel working in the EOI unit.

Tax administrations should also establish that new personnel have effectively understood their obligations

Box 12. **Example of communication of confidentiality obligations upon recruitment**

Newly recruited personnel of Jurisdiction B's tax administration sign a confidentiality and non-disclosure agreement as part of their terms and conditions of employment. In this agreement they are explicitly informed that:

- Information systems access should only be used for appropriate work activities.
- Their usage of information systems can and will be monitored.
- Inappropriate use can lead to administrative and, if the case, criminal investigations.

In addition, new personnel are given a copy of the relevant part of the Tax Code that lays out the tax secrecy obligations.

A representative from the human resources division and the senior manager of the recruiting division deliver new recruits a brief induction with an explanation of the practical interpretation of the legislation and of confidentiality and non-disclosure requirements. This induction training includes a short quiz at the end.

At the end of the induction program, new recruits take part in an official ceremony where they swear an oath of confidentiality, which they swear to maintain even after the end of the employment relationship.

and are committed to operating in a manner consistent with confidentiality and security policies. For this purpose, there should be processes and procedures to determine the effectiveness of the communication, whichever instrument or means of communication used. For example, tax administrations can communicate and assess personnel's understanding of confidentiality policies through mandatory induction programmes with testing and trainee feedback during the first week of employment. Box 12 provides an example of communication upon recruitment.

External contractors

Some services may be provided by external contractors, e.g. IT, printer maintenance, cleaning services, or contractors hired to provide specific skills such as data analytics, among others. Contractors and their personnel should understand the tax administration's confidentiality policies and be committed to their enforcement.

Relationships with contractors will normally be governed by contracts and/or Service Level Agreements (SLA), covered in more detail in SR 3.2.4.4 on supplier service delivery management:

- **Contracts** are enforceable agreements that outline the duties and responsibilities of the parties.
- **SLAs** are agreements in which tax administrations establish a minimum level of service expected from the external contractor. SLAs focus on performance measures and metrics to ensure the contractor carries out the service under the quality standards agreed to.

Whichever the type of agreement used, it should contain explicit requirements for the protection of the confidentiality and security of information, including at least:

- **Access.** Access to the tax administration's systems should be provided on a need to know basis and be commensurate with the scope of services the contractor is engaged to provide (see SR 3.2.3 for further detail on access management).
- **Incident reporting.** Contractors should report all information security incidents to the ISO as soon as possible after they occur or are discovered. There should be escalation processes if confidentiality is breached (see SR 3.2.6.6 for further detail on incident management).

SRs 3.2.2.3 and 3.2.2.4. Stage 2: Controls that relate to the ongoing employer-employee relationship

This section is about ensuring that during employment, personnel receive regular exposure to organisational requirements on confidentiality, and apply security policies and procedures in practice. This can be achieved by a combination of training and awareness, and putting in place mechanisms both to encourage and enforce compliance.

SR 3.2.2.3 therefore requires tax administrations to ensure that employees and contractors 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. SR 3.2.2.4 requires tax administrations to ensure that employees apply security policies and procedures.

Security Training and Awareness

Although training and awareness have similar and related objectives, they are nonetheless distinct concepts (see Figure 8).

Training and awareness needs, their content and frequency should be identified and defined both at the senior levels within the tax administration (e.g. ISO, senior managers of tax divisions, human resources and IT departments) and as part of the manager-personnel relationship.

Training

Confidentiality and security training should be integrated into institutional requirements and policies for the professional development of personnel. Training is a process that starts before the training event, when training needs are identified, up until personnel effectively apply the knowledge learned in their daily work. It should be delivered regularly to ensure that personnel are updated on the latest developments.

Depending on how a tax administration manages its training and professional development function, the officers leading the confidentiality and security training may vary. In any case, it is good practice to ensure the involvement and participation of the departments responsible for human resources, IT and security in the development of the content and delivery of the training.

Different categories of security training can be provided, including:

- **Base layer of security training**, by which all personnel are communicated the ISM policy and other key organisational policies relating to confidentiality and security processes, such as the Tax Code, the physical security policy, etc. This type of training can be integrated with induction training discussed above in relation to recruitment controls.

- **Role-related training**, tailored to the demands of each role. For example, personnel in the EOI unit are expected to receive special training on the processes for the handling of exchanged information, as reflected in the EOI manual or similar procedure, and be particularly sensitised to the treaty-based requirements surrounding the handling and use of information received from foreign competent authorities. Moreover, personnel in senior positions or with relevant responsibilities (e.g. ISO) might receive ad hoc training related to the particular needs of the role, e.g. certified training in security operations, cyber security, access management, etc.

- **Training not related to a specific role**, but to the environment in which personnel operate. Examples include taking care of office facilities (e.g. laptops, PCs), the risks associated with internet technologies, etc.

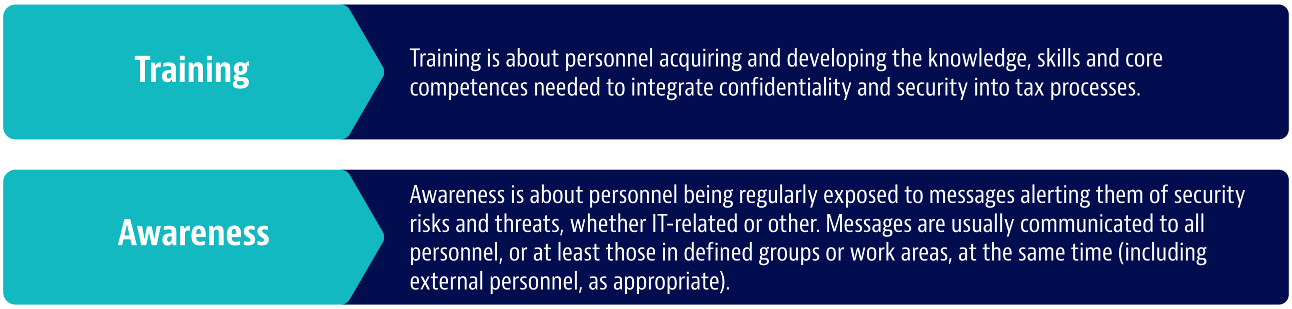
- **Training based on role changes**, e.g. when personnel are promoted to a new role.

Awareness

Awareness-raising campaigns can include:

- **Messages pertaining to IT risks and threats**, e.g. warning personnel about the dangers of opening

FIGURE 8. **Definition of training and awareness**



Training

Training is about personnel acquiring and developing the knowledge, skills and core competences needed to integrate confidentiality and security into tax processes.

Awareness

Awareness is about personnel being regularly exposed to messages alerting them of security risks and threats, whether IT-related or other. Messages are usually communicated to all personnel, or at least those in defined groups or work areas, at the same time (including external personnel, as appropriate).

links in emails from unknown sources, or of *phishing or spear phishing attacks*,[13] that may attempt to gather information that could be used to jeopardise tax administration data by triggering malicious downloads such as ransomware and spyware.

- **Messages pertaining to physical security risks and threats**, e.g. reminding personnel about the importance of always reporting the loss of a photo ID badge.

Awareness campaigns should not only focus on helping personnel avoid becoming victims of IT or other attacks, but also on educating them about their responsibilities as tax officers (e.g. always reporting phishing attacks to the department in charge and/or the ISO, so that appropriate preventive or remedial actions can be taken).

As with training, it would be good practice to involve the departments responsible for human resources, IT and security in the development and delivery of awareness campaigns. Box 13 provides an example of security training and awareness in a tax administration.

Ensuring that personnel actually apply security policies and procedures

Personnel should apply security policies in their day to day work and when utilising systems and processes that involve confidential information. Senior managers therefore need ways to assess personnel's level of compliance with security obligations. These may include:

- Including information security as part of employees' performance agreement or objectives, and covering it as part of performance management meetings between manager and subordinate.
- Clearly defining the objectives of security training events and awareness campaigns, in terms of the confidentiality needs they fulfil, and following up on their results through surveys or quizzes, team meetings and feedback to senior managers from personnel.

The role of the manager is crucial, as it is managers who will have the most impact persuading personnel to undertake the necessary training, and they can verify that personnel have gained good understanding of the training and apply it in their daily work.

[13] Phishing attacks are sent to many recipients. Spear phishing attacks are targeted to a single individual.

Box 13. **Example of security training and awareness**

All personnel of Jurisdiction C's tax administration receive mandatory information security training at least every two years, in accordance with the ISM policy requirements. Training is provided by the Institute of Tax Studies, which is part of the tax administration. Its contents are developed by the ISO in conjunction with the head of IT and the Institute, and regularly updated according to developments in the security environment and based on attendees' and senior managers' feedback. The training covers confidentiality in relation to tax processes as well as wider issues such as risks arising from the use of technology and social media, and physical risks.

An e-learning system is also available, covering the following topics:

- Tax secrecy legislation, ISM policy and Code of Conduct.
- Protecting against IT, internet, social engineering and phishing threats.
- Information classification, storage and management.
- Security incident reporting and management of data breaches.

The e-learning modules include quiz questions at the end of each section, to check personnel understand the basic requirements before they can proceed to complete the online training. Each quiz requires a 90% pass rate. The ISO and line managers verify that all personnel have successfully concluded the training and receive feedback via staff meetings.

Personnel receive daily email messages from the IT department about protecting information and information systems against internal and external threats, with examples in relation to malicious emails, password management, clear desk and clear screen policies, social engineering and internet hoaxes. These messages are also available in the intranet.

The tax administration requires contractors to provide information security training to their personnel under SLAs. Compliance with this requirement is supervised annually by the tax administration's Internal Audit team.

Box 14. Example of enforcing and assessing compliance with confidentiality policies

Jurisdiction A's tax administration personnel are regularly reminded of their obligation to protect the confidentiality of tax information, via pop-up banners, announcements on the intranet and training events. Disciplinary procedures are published in the intranet. Unauthorised access and disclosure of information are listed as major misconduct.

All personnel carrying out roles associated to the management of taxpayer information are required to include in their annual objectives at least one objective that relates to information security.

Internal audit conducts audit checks, such as reviewing system access audit logs, on an on-going basis to check if there was unauthorised access to information by personnel. The results of these audits are reported to line managers and the ISO.

When administrative or legal action is taken against personnel for breaching confidentiality obligations, such cases are publicised to staff via staff meetings and the intranet as a form of deterrence.

Disciplinary procedures and sanctions for non-compliance are also a key part of ensuring that personnel apply confidentiality and security policies. Such procedures should be communicated and reminded to personnel at all stages of the employee lifecycle.

Sanctions could be administrative, civil or criminal, depending on the seriousness of the offence. The domestic legal framework should enable the imposition of sanctions (this aspect is covered in detail in CR 3.3, which discusses enforcement provisions and processes to address confidentiality breaches).

Tax administrations should clearly demonstrate their willingness to apply sanctions when behaviour falls below the standard required, and where the safeguarding of information is concerned. It is essential that personnel see that good information security behaviour and performance will be rewarded, and poor practice will be challenged and punished as appropriate. Box 14 provides an example of enforcing and assessing compliance with confidentiality policies.

SR 3.2.2.5. Stage 3: Controls that relate to the termination of employment

SR requires that tax administrations have human resources policies and processes relating to the termination of engagement that protect sensitive information. This refers to defined procedures relating to the termination of employment, whether on retirement, resignation or cessation of all types of personnel, including contractors. Some tax administrations may also consider a change of position as termination of employment in the previous role, and the controls described in this section can be used in such scenario, as appropriate.

The controls need to ensure that the confidentiality of the information is maintained beyond employment, and essentially cover the following aspects (see Box 15 for an example).

Recovery of official property or assets

There should be a process for checking that all official property (e.g. ID badges, laptops, mobile phones, USBs, etc.) have been returned by departing personnel (this process is linked to SR 3.2.4.3, on asset management).

Line managers and/or areas in charge of asset management or human resources should be in charge of the process. The process can be implemented, for example, in the form of a checklist signed by the departing personnel, sometimes in the context of an "exit meeting".

Removal of rights

Removal of rights refers to the timely withdrawal of all access permissions, whether physical (access to buildings, offices) or logical (access to systems). The process to establish physical access requirements and to provision and de-provision logical access is described in detail in SR 3.2.3, on access management.

Personnel normally have access rights to private working areas of the tax administration and some may have special access rights to areas where access is more tightly controlled (e.g. data centres or file stores). Access to these areas may be enabled through photo ID, electronic passes, biometric identification, security codes, etc., depending on the physical security requirements of the different premises.

Information Security Management framework that adheres to internationally recognised standards or best practices (Core Requirement 3.2)

For departing personnel, all these access permissions should be withdrawn by requiring them to surrender their photo-ID badges, deactivating their biometric identification and security codes, etc. This process usually involves senior line managers, physical security management and/or human resources.

Tax administrations should also have processes to timely de-provision logical access to systems. This process is critical in terms of information security, as a very significant cause of data breaches is the hacking of unused access rights.

The usage of logical access rights therefore needs to be tightly controlled. The removal of access rights should be arranged in advance of the last day on which those rights are needed, and rights should be withdrawn at the end of that final day. The responsibility for de-provisioning logical access should lie with the senior managers responsible for the relevant tax business process or application, with the technical support of the IT department, as those senior managers are the ones in charge of determining the access criteria and approving access rights to the system.

When personnel are leaving or being suspended because of misconduct, the process should enable all rights (physical and logical) to be withdrawn immediately if an appropriate request is made (e.g. from senior or line managers, or the investigations department).

Clarity of future obligations.

Tax personnel acquire a lot of knowledge about sensitive information related to taxpayers and their tax affairs. Its confidentiality should be maintained beyond employment. This obligation should be made clear to departing personnel, and should be recorded in a formal document signed by personnel and a relevant manager (e.g. the document also covering the return of assets).

SUB-REQUIREMENT 3.2.3: ACCESS CONTROLS, INCLUDING PHYSICAL AND LOGICAL ACCESS

SR 3.2.3 is about protecting confidentiality by ensuring that only those users that have a legitimate business reason to access information are allowed to do so.

International ISM standards require tax administrations to have overarching access management policies covering all accesses (reflected in SRs 3.2.3.1 for physical access, and SR 3.2.3.3 for logical (IT) access).

Box 15. **Example of controls upon termination of employment**

In Jurisdiction B's tax administration, departing personnel's system accesses are automatically revoked by the IT department based on the service termination date provided by human resources. Where appropriate, such as in cases of misconduct, access is terminated at an earlier date.

An exit interview is carried out on the last day of employment. The person's supervisor, a representative from human resources, and a representative from physical security management are present. Personnel are required to sign a document stating that all official property and assets have been returned, and that they are bound to a lifetime of secrecy in relation to all confidential information learned while employed in the tax administration. The document also states that a breach of confidentiality provisions will be penalised under civil or criminal law, and counsels the departing personnel to avoid placing themselves in positions that could raise conflicts of interest in the maintenance of confidentiality obligations.

Also as part of the exit interview, a checklist verification is undertaken to verify the recovery of all official property and the removal of all rights. This checklist includes:

- Collecting the personnel's pass, security tokens and keys which have been issued for system and physical access to classified information.
- Collecting their laptop and official mobile phone.
- Collecting all classified information assets and materials issued to them to carry out their work.
- Verifying that access to IT applications and restricted office premises has been removed.
- Verifying that the person's email account has been deactivated.
- Informing relevant stakeholders (colleagues, etc.) of the departure.

Tax administrations should then have arrangements to adequately implement and administer those policies, i.e. adequately protecting physical premises and having defined internal and external perimeters (SR 3.2.3.2)

Table 10. **Glossary of main concepts**

Concept	Description
Access controls	Security controls that ensure that access to information, physical premises and systems is based on need to know and minimum rights.
Access management	Policies, processes and procedures, owned by senior management and not solely by the tax administration's IT function, that govern physical and logical access, and effective processes for the provisioning and auditing of logical access and for the identification and authentication of users.
Access provisioning	Effectively granting access to information through the creation of user accounts, password management, and by assigning specific access rights and authorisations to users.
Authentication	When a user accesses IT systems, the authentication process ensures and confirms a user's identity in a non-repudiation based manner.
Authorisation	Once a user is authenticated on a system, the user is then authorized to access resources based on need-to-now and least privilege principles.
Identification	A process used in IT systems to uniquely identify the users who have an access right.
Least privilege	Access management principle that establishes that legitimate access should be restricted to the minimum specific functions that the users need to do their job.
Legitimate user	User who gets a specific access right based on the need to know and least privilege principles.
Logical access	An access to systems through identification, authentication and authorisation processes.
Need to know	Access management principle that establishes that taxpayer information should only be accessed by personnel with a legitimate business reason to do so.
Physical access	An on-site access to specific areas.

and arrangements to effectively provision logical access as defined by business managers, and not solely the IT department (SR 3.2.3.4).

This section provides guidance on the definition of policies and their implementation. Table 10 provides definitions of the main concepts covered in SR 3.2.3.

There are three parts to this SR:

- Overarching principles of access management.
- Guidance on physical security in tax administration premises (SRs 3.2.3.1 and 3.2.3.2).
- Guidance on putting in place a logical access policy and controls (SRs 3.2.3.3 and 3.2.3.4).

This section is not intended as a full exploration of the subject of access management. It highlights generic aspects likely to apply to all tax administrations and considered to be central to access management in a tax administration context.

Overarching principles of access management

International standards on access management are governed by two principles, which should be applied without exception (see Figure 9):

- **Accesses should be controlled based on the need-to-know principle**, meaning that taxpayer information should only be accessed by personnel with a legitimate business reason to do so. This principle contains a further principle, called least privilege, according to which legitimate access should be restricted to the specific functions that the users need to do their job. The application of these principles gives taxpayers assurance about the protection of their privacy rights and thus about communicating openly with the tax authorities.

Information Security Management framework that adheres to internationally recognised standards or best practices (Core Requirement 3.2)

- **Accesses (physical and logical) should be logged**, identifying the unique individuals that accessed the premises or the information, the time and duration of the access, and details of the action taken. The application of this principle makes it easier to trace actions back to the relevant persons, and in turn, provides strong disincentives against unlawful or inappropriate actions.

FIGURE 9. **Principles of access management**

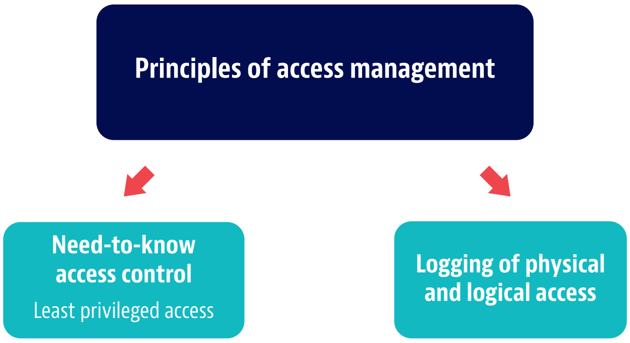

Principles of access management
Need-to-know access control
Least privileged access
Logging of physical and logical access

Table 11 indicates the types of users which may legitimately access information in the tax administration context.

SRs 3.2.3.1 and 3.2.3.2. Physical access security

This section is about the policy approach to physical access security at each of the different premises in which tax administrations operate, as well as the procedures and controls to ensure its effectiveness.

Turning physical security into policy(ies)

Physical access to tax administration buildings should be articulated in terms of a physical security policy or policies endorsed by senior management. SR 3.2.3.1 therefore requires tax administrations to have a physical access control policy owned by senior management. SR 3.2.3.2 requires tax administrations to adequately protect physical premises and have appropriately defined internal and external secure perimeters.

Policies should be consistent with the size and complexity of the tax administration and should guide those who are responsible for managing physical security at each of the different locations from which the administration operates.

Physical security policies can be framed in terms of security design of physical premises, user requirements, and the specific controls in place to manage access.

Security design of physical premises

Policies should define the range of locations, premises, and offices in which the tax administration operates, and

Table 11. **Categories of legitimate users**

User	Description
Tax administration personnel	Personnel who because of their role are directly involved in the handling of taxpayer information. This may include personnel from the EOI unit and certain compliance divisions charged with risk analysis and inspection activities that utilise exchanged information, e.g. large business and international division, offshore compliance division, high net worth individual division.
IT external contractors	Personnel of IT suppliers who manage services on the tax administration's behalf, such as those administering the systems and databases in which taxpayer information, including exchanged information, is contained, and that have also been subject to appropriate background checking and vetting processes.
Supervisory authorities	Courts, administrative bodies and oversight bodies involved in the assessment, collection, enforcement, prosecution, and determination of appeals in relation to the taxes, including with respect to information exchanged under an international agreement. Some countries have implemented systems of legal information gateways whereby data is shared with specified and authorised supervisory authorities.
Taxpayers and agents	Information can also be disclosed to taxpayers concerned and their authorised representatives (e.g. agents). Modern technology is enabling jurisdictions to introduce taxpayer self-service arrangements, under which taxpayers not only self-submit a tax return, but also manage payments and manage other aspects of their tax affairs.

determine their physical security requirements based on the different types of users that will need access to those various premises.

The main design consideration when framing physical security policies should be to protect information from those who do not need access to it. For this purpose, international good practices to consider are:

- Arranging premises in a way that enables the separation of “trusted” users (employees, contractors) who are entitled to access more restricted or inner parts of the premises from others.
- Organising building and premises space to support the principles of need-to know and least privilege, and enabling physical separation for more sensitive work areas or where critical activities take place (e.g. data centres or where particularly sensitive tax data is handled, with access only for those with higher levels of clearance based on higher levels of trust, such as the EOI unit).

Types of users and their requirements

Different types of users with different levels of access rights should all have their own requirements and sets of controls to ensure they only access to the premises for which they have a legitimate purpose.

Defining user requirements involves assessing who needs access, to what, and why. The main categories of users may include:

- Personnel of the tax administration with the right to access the private areas of buildings.
- Personnel with access to buildings such as the data centre where access is more tightly controlled.
- Personnel from other government departments.
- IT and non-IT contractors providing services, e.g. cleaners.
- Taxpayers and tax agents visiting to discuss tax matters, or members of the general public.

If the tax administration is located on premises it does not own, the building may have other types of particular users with their own security requirements.

Controls to manage physical access

Policies should include a structured set of physical security controls applied within the tax administration. To ensure these controls meet good practice standards, they should be risk-based and linked with the physical design and user requirement considerations.

Table 12. **Example of physical security matrix**

Premises	User types	Controls
Main entrance	Tax administration personnel, IT contractors	CCTV in real time, security guards, screening of personal effects.
	Other government authorities	
	Taxpayers	
Internal offices	Tax administration personnel, IT contractors	Electronic passes with photo-ID, turnstiles, CCTV.
	Other government authorities	Temporary passes with ID, turnstiles, CCTV. Escorting at all times by tax administration personnel.
EOI unit / File stores	EOI unit personnel	Electronic passes with photo-ID, turnstiles, CCTV, intrusion detection and alarm system, keypad entry locks, multifactor access to IT devices.
Data centre	IT administrators	Electronic passes with photo-ID, turnstiles, CCTV, intrusion detection and alarm system, keypad entry locks, multifactor access to IT devices, air conditioning, fire protections.

Box 16. International good practices in the framing of physical security controls

Physical security controls should be structured in a logical manner. A logical approach would be to use an "out to in" approach starting with the outermost control as a person approaches a building, and working inwards towards users' workstation. This approach would consider the following:

- What is the outermost perimeter? Is it the land surrounding each building, including any parking areas? Is access to the parking area controlled, and if so, how? If the land is fenced with gates, then are these guarded? Are there secondary control systems such as CCTV, and is it monitored in real time?
- Is there a proper inventory of the various locations (e.g. doors, fire doors) through which users may access or leave the building? Is there a clear statement for each door type as to how it should be used and by whom? (e.g. personnel access, taxpayer access, or both, fire exit, deliveries access point).
- Most buildings will have an entrance area, often a location where both personnel and others mingle. How do the different building users gain access? Do they need an electronic pass? How are passes (electronic or not) issued and controlled? Do they include a photo? If there is no photo, are there any other ways of checking that the holder is the legitimate user?
- What are controls in other public areas within buildings, such as public enquiry counters?
- How is access gained to private areas of a building, for example by swiping an electronic pass? Must users pass through a full height turnstile (i.e. a control that limits access to one person at a time)? If not a full height turnstile, are there any secondary controls, such as security guards? Or CCTV? If CCTV, is it monitored in real time?
- Within the restricted areas of a building, how would personnel know whether other people have a right to be there?
- What are the rules pertaining to the management of physical security within individual work areas within buildings?
- What are the controls in areas where more sensitive operations are handled? (e.g. data centres, file store)
- What type of controls are employed generally within a building? For example, is CCTV used and, if so, for what purposes? And how is it monitored? It is important to note that CCTV cameras should not be positioned in such a way that they can view desks, PC screens, file-stores, etc., or anything that might lead to taxpayer information ending up on the CCTV system.
- Is there public space around the building (nearby buildings, houses) that could be used to impair confidentiality, and what are the controls applied in this regard?

An alternative approach?

Another approach might be to split the control list into:

- Baseline controls that constitute the set of minimum controls.
- All of the additional or enhanced controls that are applied as a response to a specific risk or concern.

A full list of controls may be set out, for example, as a matrix listing different building zones or access types, user types, what access rights they have, and the relevant controls. Table 12 shows a simplified example of a physical security matrix, and Boxes 16 and 17 provide more detailed guidance and examples of approaches to consider when framing physical security controls.

Testing physical security controls

There should be a system for testing whether the security controls laid out in policy are being correctly and effectively implemented in practice.

Improvements to controls should build on earlier testing conducted in accordance with testing plans. In turn, testing plans should be re-developed as needed, building on the findings of the existing plan.

In general, when assessing or testing physical security controls, the following aspects should be considered:

- Physical security assessments should be periodical and updated based on the findings and lessons learned from previous assessments and/or incidents, with a combination of random and risk-based tests.

Box 17. **Example of assessment of physical security controls**

The Physical Security Management division of Jurisdiction A's tax administration checks at least once a month that physical controls are working. This includes technical checks of entry locks, alarms and surveillance cameras. Physical security is audited once every three years by an external service provider.

All physical access control system failures are reported to Physical Security Management. If there is evidence of inappropriate access to premises, this triggers an investigation to determine if there has been material damage (e.g. stolen or damaged property) or a possible breach of data (paper or digital). The findings and conclusions of the investigation are documented and used to remedy the control failure that caused the incident.

Data centres are guarded and have an electronic access control system requiring biometrical identification. Reports containing data centre access logs are reviewed every two weeks. Data centres have distinct video surveillance systems.

- Physical security incidents and events should be reported promptly to building managers, logged and documented (incident management controls are described in more detail in SR 3.2.6.6). If incidents are not being appropriately reported and logged, it could give the false impression that the system is working. There can be many types of incidents, with different levels of severity and impact, such as employees losing their security pass, attempts to gain inappropriate access to buildings, people moving from one area to another without swiping passes, theft of official material, etc. Personnel should be aware of the importance of reporting an incident, and the reporting format should document its details so that appropriate actions can be taken.

- Assessments of controls of critical sites (e.g. data centres, EOI unit, file store) should take into consideration the possibility of using additional controls commensurate with the classification of information handled in those offices (see SR 3.2.5.1 on protection of information) and institutional risk assessments (see SR 3.2.1.4 on risk management).

SRs 3.2.3.3 and 3.2.3.4. Logical access

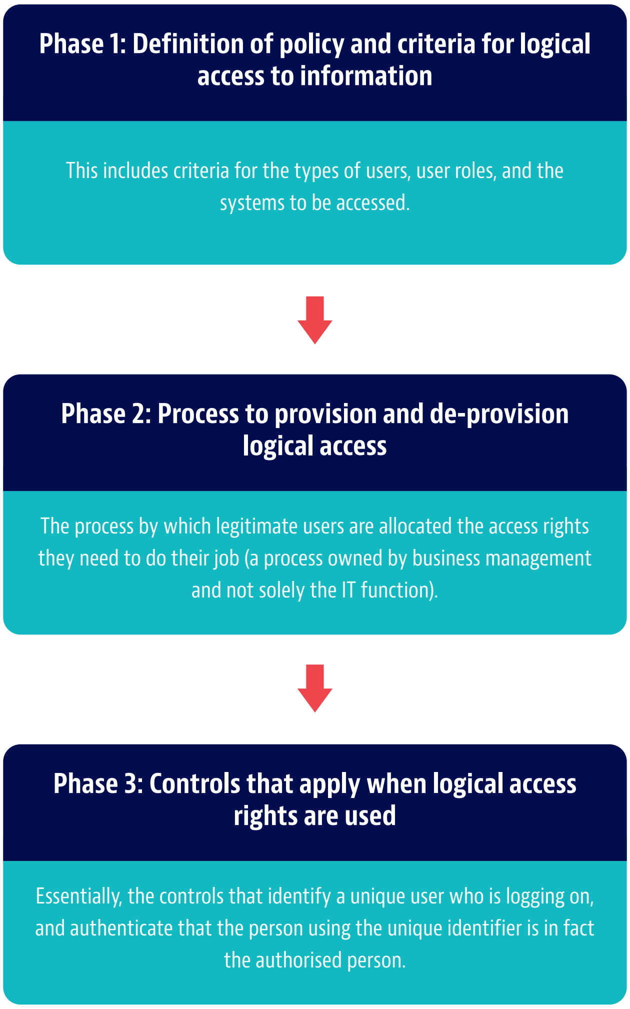
This section is about the overall approach to design and test appropriate logical (IT) access controls for data held electronically in various information systems.

SR 3.2.3.3 requires tax administrations to have a logical access control policy owned by senior management and based on the need-to-know and least privileged access principles. SR 3.2.3.4 requires them to have policies, processes and procedures, owned by senior management and not solely the organisation's IT function, that govern logical access, and effective procedures for the provisioning and auditing of logical access and for the identification and authentication of users.

Phases of logical access management

The requirements are generally reflected in three phases of logical access management, as shown in Figure 10:

FIGURE 10. **Phases of logical access management**



Phase 1: Definition of policy and criteria for logical access to information

This includes criteria for the types of users, user roles, and the systems to be accessed.

Phase 2: Process to provision and de-provision logical access

The process by which legitimate users are allocated the access rights they need to do their job (a process owned by business management and not solely the IT function).

Phase 3: Controls that apply when logical access rights are used

Essentially, the controls that identify a unique user who is logging on, and authenticate that the person using the unique identifier is in fact the authorised person.

Table 13. **Definition of policy and criteria for logical access to information**

Considerations to inform the definition	Who defines the criteria for information system access
● The logical access policy should express the need-to-know and least privilege principles, i.e. establish that users should only have the access rights they need to do their job or fulfil their role, and that legitimate access should be restricted to the specific functions users need. ● When user role types are different for different tax processes, there should be adequate controls in place to ensure consistency of criteria across systems. ● Access rights may depend on where the data is stored: data centres within tax administration premises, outsourced datacentres, or in the "cloud". [14] [15] ● There may be access rights and policies in relation to the use of IT applications such as e-mail and internet browsers for non business purposes. ● There may be access rights in relation to working outside of the office environment, particularly secure access to confidential data when working outside of the Local Area Networks within the tax administration offices.	The criteria for logical access to information should be determined by the persons responsible for the business process that uses the relevant tax application, and endorsed by senior managers of the tax administration. It is the senior managers who are accountable for the operation of tax administration systems, so they should be the ultimate arbiters of how the access controls are designed. For example, the senior tax officer in charge of the management of the AEOI system should be responsible for determining the access criteria for that system. If access management controls are too lax then confidentiality could be compromised, and if the controls are too tight then business efficiency could be impaired. As with many security issues, there is a fine balance between confidentiality and availability. The consequences of getting that balance wrong are business consequences, not IT consequences. Nevertheless, it is good practice to develop the criteria collaboratively with the IT department. The IT department has a technical understanding of the pros and cons of providing access, and specific areas where restrictions are likely to be needed: for example, those with high access privileges, such as administrator roles. Administrators are users usually responsible for the administration of IT infrastructure within the tax administration network, and should not normally have internet access, including email, as part of the administrator role.

Phase 1: Definition of policy and criteria for logical access to information.

Table 13 summarises the definition of the criteria for logical access to information.

Phase 2: Process to provision and de-provision logical access

Provisioning logical access

Once the criteria for logical access rights have been determined, the next phase is to effectively provision access to information, i.e. grant users the access rights pre-determined for their type of role (see Box 18). Provisioning logical access is relevant in circumstances that include:

- When new personnel are recruited and require access.
- When personnel change job or role (e.g. a tax officer moves from a project division to a compliance division and therefore needs access to taxpayer information).
- When personnel have new functions or responsibilities added to their role (e.g. a senior manager is charged with managing corporate taxpayers as well as individual taxpayers).
- Ad hoc access requests for particular roles.

This list is not intended to be exhaustive and there may well be other circumstances to consider. In any case, as part of provisioning logical access, tax administrations should determine all of the different circumstances in which logical access to IT applications, systems or services may need to be provisioned.

[14] Details of the controls applied when external supplier services are used are described under SR 3.2.4.4.

[15] Government departments are increasingly considering the use of so-called "Cloud" services instead of data centres controlled by the department itself.

Box 18. **Why is effective provisioning of logical access so important?**

Effective access provisioning enables tax administration personnel to timely acquire the legitimate access rights they need to do their jobs. If, however, there is not a clear route to achieve this, personnel could potentially create ad hoc access processes that will enable them to carry on working. Such ad hoc processes are unlikely to be consistent with security and confidentiality principles.

As a hypothetical example, Jurisdiction B's tax administration has not established formal procedures, controlled by senior management, for provisioning role-based access. Instead, there are manual and ad-hoc practices between business divisions and the IT department for the granting of specific access rights. In some cases, when personnel need a certain access, they simply email an IT colleague who grants it without managerial involvement. In other cases, the access request is first approved by the staff's manager before it is submitted to the IT department, but includes rights that are not necessary for the staff to fulfil their job duties. No audit trails of the access granting process are kept in these cases. During an assessment of confidentiality standards, this jurisdiction would be recommended to develop and enforce a formal access management process, along with the formal procedures for the provisioning and de-provisioning of logical access rights.

De-provisioning logical access

Another critical requirement is the ability to withdraw, or de-provision access rights (see example in Box 19). The hijacking of access rights is recognised as a significant cause of data breaches. Tax administrations should therefore take appropriate precautions to ensure that the only system accesses available at any point in time are those required by legitimate users. The situations that de-provisioning arrangements are expected to cover would include:

- **Departing personnel.** Access rights should be withdrawn by the last working day, if not before. Where people are leaving in specific circumstances such as misconduct, access rights should be capable of being withdrawn immediately.
- **Change of job or role.** Access rights should be withdrawn as soon as the old job is concluded and at the same time, or before, new access rights are given.
- **Temporary withdrawal.** For example, if personnel take long periods of recreational or sickness leave, or when investigations of misconduct are being carried out.
- **Unused access.** Access rights that are not being used should be de-provisioned.
- **Time-limited access.** There should generally exist the capability to provision access on a time limited basis, so that the process automatically de-provisions access after a certain period of time expires (and there may exist a linked process for restoring access promptly, as needed).

Procedural controls once logical access has been provisioned

After access to systems is provisioned, adequate procedural checks should be carried out to ensure that only legitimate users do in fact have the access rights (see example in Box 20). Procedural checks may include:

- Periodical checks by dedicated personnel, supervisors, or the senior managers who approved the access request, to verify that:
  - The persons shown as having access rights are in fact legitimate users.
  - The persons who have been given access are in fact current users (for example, that they still have that role or that they have not retired).
- Periodical checks by the internal audit function.

Phase 3: Controls that apply when logical access rights are used

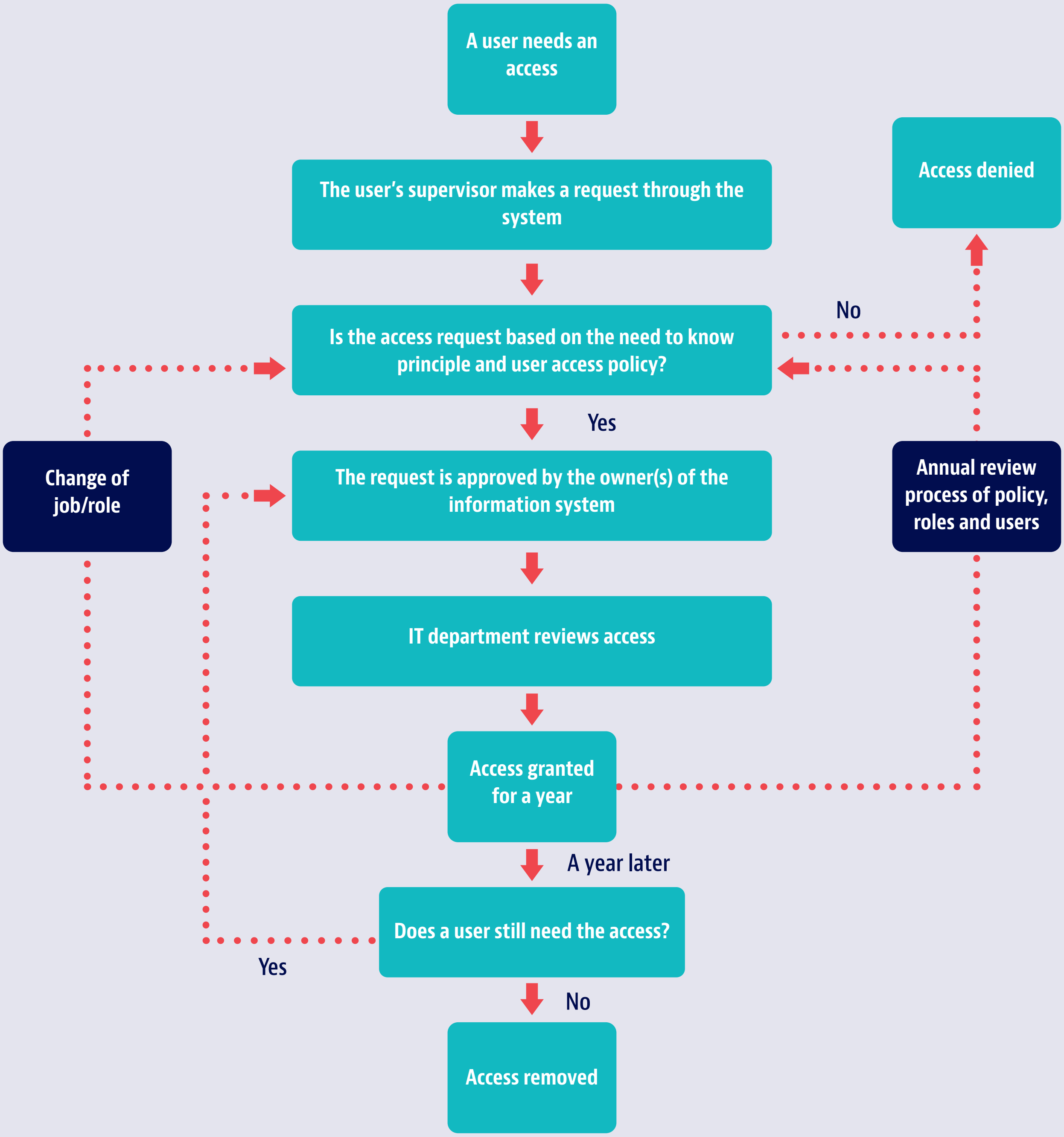
After users are given access rights to information systems, they will need to access or 'log on' to those systems. Tax administrations should ensure that users are uniquely identifiable and authenticated on each occasion that they access a system.

Information Security Management framework that adheres to internationally recognised standards or best practices (Core Requirement 3.2)

Box 19. **Example of provisioning and de-provisioning of logical access**

In Jurisdiction C's tax administration, users' access to various information systems are predefined based on job role, and based on the "Policy to Provision and De-Provision User Access in Tax Administration C Systems". Granting users' accesses requires approval from their supervisor (at minimum, head of unit). Then, accesses must be endorsed by the respective information system owners, and only senior management can be appointed as system owners. Following approval by such owners, the access is reviewed and granted by the IT department, as part of a final technical check.

The following figure shows an example of a provisioning and de-provisioning process:


A user needs an access

The user's supervisor makes a request through the system

Is the access request based on the need to know principle and user access policy?

The request is approved by the owner(s) of the information system

IT department reviews access

Access granted for a year

Does a user still need the access?

Access removed

Access denied

Change of job/role

Annual review process of policy, roles and users

Box 20. **Example of logical access procedural controls**

Jurisdiction A's tax administration has appointed a team of access rights coordinators to review the rights granted to all users, both employees and contractors. After rights have been granted, coordinators send confirmation emails to supervisors and senior managers to verify that they in fact approved the access requests. This coordination team also checks periodically that all access rights are valid, and that all obsolete accounts and accesses are removed. These checks are reported, reviewed and endorsed by the senior tax manager in charge of the information system, and the human resources department. The frequency of the checks varies based on system classifications, but they are performed at minimum every six months.

Identification

All users of IT systems should have a unique identifier(s), to conform with the principle that all actions can be linked to identifiable individuals.

It may be possible for a user to have multiple identities, e.g. if they have access functions with different levels of privilege, but these identities should still be unique to the user concerned. Where, very exceptionally, it is not possible to use unique identifiers, there should be compensatory controls in place, e.g. a combination of a control log together with managerial authorisation.

Authentication

The identification should be augmented with authentication requirements. The standard form of authentication is a password, or series of characters known only to the person who bears the unique identifier. Box 21 outlines some international good practices on password and user account management.

Other forms of authentication requirements, in addition to passwords, can be used. An example is the use of workstation identifiers. Workstations (PCs, laptops, etc.) issued by a tax administration with unique identifiers can be used to gain additional assurance as part of the authentication process. For example, requiring the unique identifier of the PC or laptop to be entered following the user's password, in order to get access. Although making this type of link can be a useful way of gaining greater confidence in the authentication process, it can also be operationally restrictive to tie users to their own machine. This factor should be considered before deciding to use workstation identifiers, or other additional authentication options.

Multi-factor authentication

There may be special situations where additional authentication controls or "multi-factor authentication" are required. There are three types of authenticators: something you know, e.g. a password, something you have, e.g. a token, and something you are, e.g. a fingerprint. Tax administration should choose at least two out of the three authenticators to implement multi-factor authentication.

Situations that may require multi-factor authentication can include:

- **Sensitive data.** In the case of sensitive data, e.g. exchanged information, tighter authentication

Box 21. **International good practices on password and user account management**

Password management. Practices can include constraints or minimum standards on the type and numbers of passwords that can be used, restrictions on the number of repeated password failures, and requiring changing passwords periodically. For example, password minimum length of at least 10 alphanumeric characters, locking the account after 5 failed login attempts, and changing passwords every 90 days or less.

Session management. Practices can include locking PCs if not in use, and back-stop procedures to protect information if users do not lock machines. For example, PCs can be set by default to time out and prompt for user re-authentication after 10 minutes of user inactivity.

Inactive accounts. Practices can include monitor account usage and deactivating accounts if not in use. For example, accounts that have not been signed on for at least 30 consecutive days will be disabled.

controls may be necessary. These might include standard two-factor authentication (e.g. very strong password, coupled with a security token or biometrics) but could also be further reinforced by additional authentication controls, e.g. linking the user to a particular workstation (PC, laptop, etc.) located in a very secure room. Whichever the additional controls used for sensitive data, the level of control should always be based on a rigorous risk assessment, and should balance the need for confidentiality with the need for availability.

- **Administrators.** For users working in the IT department who have privileged administrator access to IT infrastructure and systems, often known as "administrators" or "super users", additional authentication controls will generally be warranted. International good practice for this type of user is to have at least two-factor authentication plus additional controls that can include:
  - Granting privileged access for a limited period, so that the access right is regularly checked and performance is reviewed before being re-established for a further period.
  - Assigning privileged users to work in pairs, thereby checking each other's actions.
  - Using commercial off-the-shelf packages that specifically focus on managing privileged access.
- **Remote access by users.** Access to taxpayer information is tightly controlled, and outside of the office it is limited only to specific functions and types of system access. When allowing external access to sensitive data, the risks should be effectively measured and mitigated. The main challenges are not technical – as there are very effective ways of encrypting information – but about a user's access to their device (e.g. laptop or tablet) being effectively controlled.

SUB-REQUIREMENT 3.2.4: IT SYSTEM SECURITY

SR 3.2.4 is about protecting information by protecting the infrastructure (both software and hardware) in which information is stored, and through which it is employed and used. The protection of information itself is addressed in the next section, SR 3.2.5.

Under SR 3.2.4, tax administrations are expected to:

- SR 3.2.4.1: Make security an integral part of providing IT services to support business functions, have a security plan for business applications, and harmonise their systems with security.
- SR 3.2.4.2: Deploy an appropriate range of IT security controls.
- SR 3.2.4.3: Adequately manage their IT assets.
- SR 3.2.4.4: Appropriately manage the delivery of services by suppliers.
- SR 3.2.4.5: Assure the continuity of IT services and its resilience to failures.

Table 14 provides definitions of the main concepts covered in SR 3.2.4.

SR 3.2.4.1. Make security an integral part of providing IT services

IT systems do not exist in a vacuum: they support the efficient management and automation of tax administrations' operations and business processes. Therefore, all IT functions, including those managing information security, should be closely aligned with the needs of the operations and business processes they support. Tax administrations should then make a decision on how to implement IT security.

Aligning IT and security with business functions

To achieve alignment, during IT design processes there should be a good level of engagement between the IT function, and tax business managers and users. The tax administration should therefore identify persons responsible for ensuring communication between those stakeholders. Without such engagement, IT systems may not achieve what business processes require them to, which could in turn create problems that jeopardise the confidentiality and integrity of information.

Integrating security into IT, and aligning IT with business, require a well organised IT department. An IT department should:

Table 14. **Glossary of main concepts**

Concept	Description
Asset management	Process that ensures that the tax administration's assets are identified and tracked from their creation or procurement to their destruction or disposal.
Baseline controls	Set of minimum security controls that a tax administration applies to certain risks, regardless of their severity.
Firewall	Equipment placed on strategic points of a network (usually those facing external or internet access and internal separated zones) that allow or block traffic based on rules.
IT security control	Administrative, technical or physical measure implemented to mitigate an IT risk.
Malware	Malicious software. Program created to exploit a vulnerability in a targeted system in order to harm it or steal information.
Outsourcing	Recourse to an external provider for the provision of goods and services.
Penetration testing	Penetration testing simulates the actions of a hacker against the organisation.
Recovery	Refers to restoring services and business operations in case of high failure.
Resilience	Refers to mitigating the risk of service interruption and ensuring tolerance to failures in services by providing continuity of service up to a certain point.
Service Level Agreement	Agreement that sets the minimum level of service an entity providing a service must comply with.
Supplier management	Risk-based process that ensures that an external supplier accessing a tax administration's data or premises does not put at risk confidentiality and security.

- Identify and define its functions, by clearly defining functional perimeters (e.g. quality, development, and support).
- Identify the key contact persons in the business departments.
- Regularly meet with business department stakeholders.

An organisational chart (see example in Figure 11) showing the communication flows between the IT department and other areas (including governance, security and business units) will help identify who is supposed to establish and communicate security requirements for business processes, and the IT solutions that support these.

Many variables influence how tax administrations structure their IT function, how it supports business functions, and how IT security controls are implemented (see Table 15).

Whichever IT organisation is used, its effect on IT and information security risk management should be considered. This consideration should lead to the implementation of appropriate governance structures and processes that ensure integration between IT security and the tax administration's day to day operations. Tax administrations should also establish clear procedures that ensure the prioritisation of security aspects when implementing IT projects, including the specific body or persons responsible.

Implementing IT security

Having decided upon an appropriate structure that integrates IT security, a tax administration will also have to make decisions on the implementation of IT systems and security. The questions that will need to be considered include:

- Will IT services be developed in house, outsourced, or both (both in terms of IT applications and systems)? (see Box 22).
- Who will decide, and who will be responsible for different IT services?
- How will it be ensured that security assessments in the development or acquisition of IT services and applications will be properly carried out?
- How in practice will security be built into IT (i.e. into the design of IT environments, development of new systems, changes to existing systems, as well as into the underlying infrastructure)?

A key process to achieve integration between IT systems, security and business systems is change management, covered in more detail in SR 3.2.6.5. System changes can open additional risks or negatively impact the effectiveness of security controls that are already implemented. Change management therefore ensures that IT system design and change are controlled processes, with security requirements in mind, and incorporating an adequate assessment of impacts.

SR 3.2.4.2. Deploy an appropriate range of IT security controls

Tax administrations should deploy IT security controls informed by the various inputs that help determine what controls are applied, and how they are applied. Inputs include information obtained from incident and problem

FIGURE 11. **Example of organisational chart showing communication flows between the IT department and other areas**

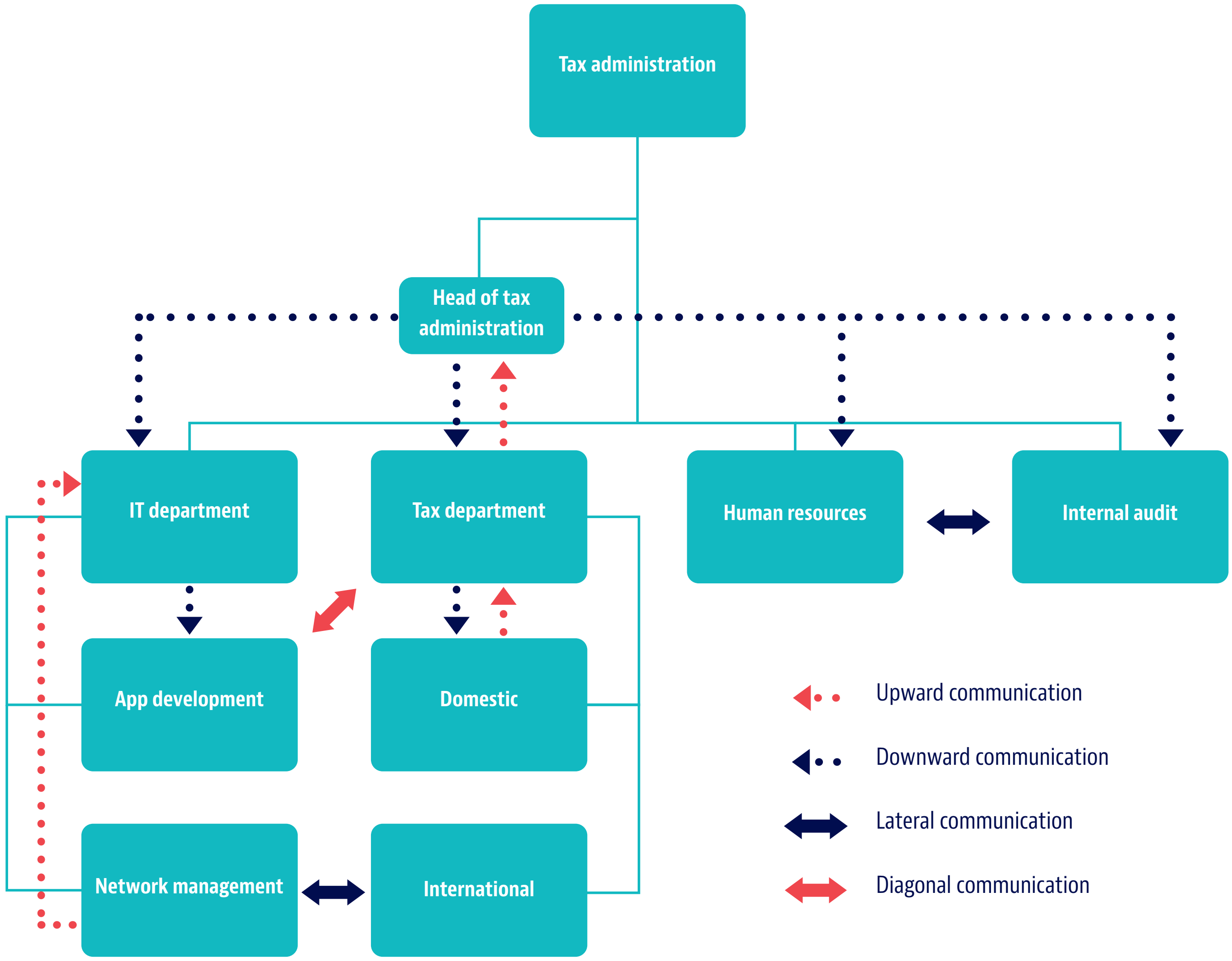


Table 15. **Examples of variables influencing how an IT function is structured**

Size of the tax administration	Outsourcing of IT functions	Lifecycle approach	IT system harmonisation
In large or more complex administrations, the IT function could include many different activities, including IT architecture, design, development, project management, release management, operations, service management, and IT security management. These could be structured as sub departments. In smaller administrations, however, there may be a single department handling all activities. Some or all activities and the associated technical decisions could be outsourced, e.g. through the acquisition of off-the-shelf IT solutions.	The IT department itself could be operated outside the tax administration. For example, a separate IT function under the Ministry of Finance, which provides IT services for all ministerial departments. In other cases, some or all IT department functions could be outsourced to private companies, including the provision of desktop services.	The activities that support the provision of IT services may be structured in IT lifecycle terms, with dedicated teams for each part of the lifecycle (e.g. design, development, release and operations). The structure could set out how the different teams of the IT department responsible for each part collaborate between themselves, as well as with business units and users of IT.	Integrating information security into the provision of IT services might be simplified if IT systems are harmonised so that a few solutions, but the same across the infrastructure, are used. Tax administrations with a high degree of harmonisation may find that it helps reduce costs and handle security issues. Harmonisation might also apply to mobile devices and equipment connected from outside the tax administration (e.g.: teleworking and personal mobile equipment accessing the tax administration's network).

management (SR 3.2.6.6), vulnerability management (SR 3.2.6.4), and most importantly risk management (SR 3.2.1.4).

Depending on how the IT function is structured, the approach to deploying controls may be more or less formalised or documented. Whichever the approach, it should be clear, within the IT function and the tax administration, how the various inputs contribute to the decisions to apply IT controls. This provides traceability for the members of the IT team charged with managing the controls. Those persons also need to clearly understand the impacts of any system changes, so that they can act accordingly to make sure that the existing controls are still operating properly.

As shown in Figure 12, IT security controls (and security controls generally) include:

- **Baseline controls**: Minimum controls applied as a result of the tax administration's initial identification of specific risks, regardless of their severity.

Box 22. **Possible advantages and disadvantages: in-house vs. outsourced IT service development**

In-house development

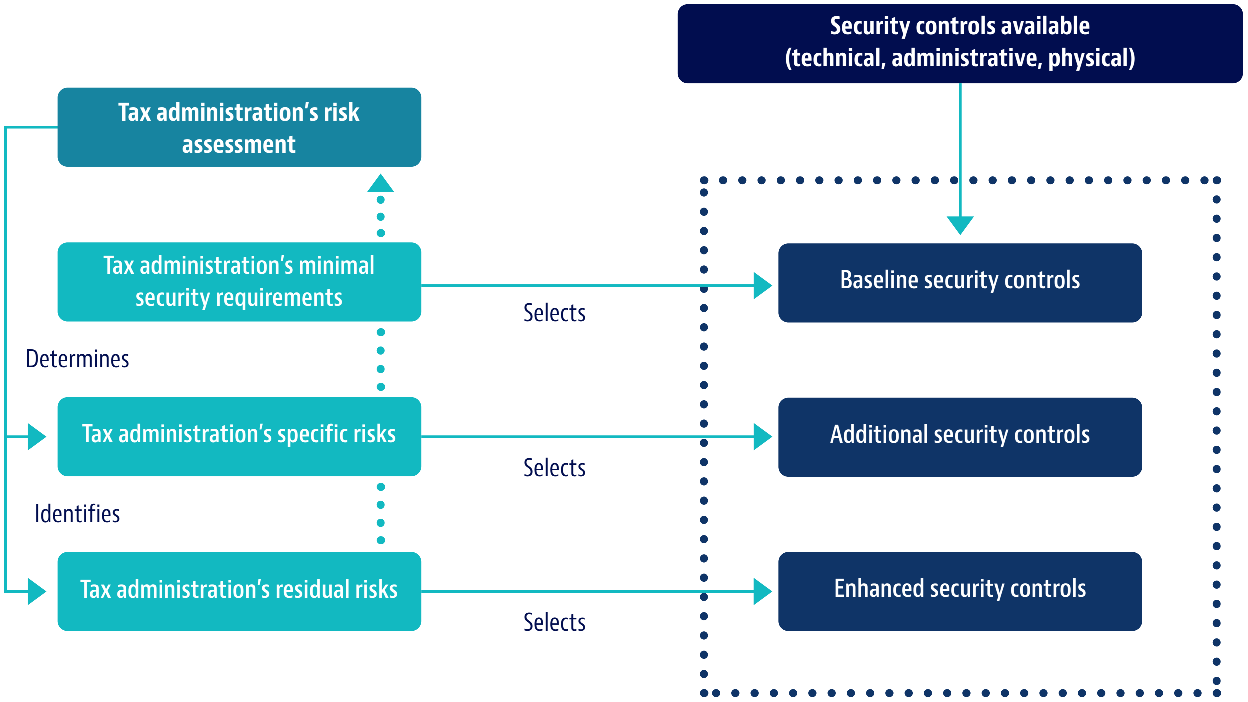
Advantages may include better internal control of IT services, better trust relationships and confidentiality. Disadvantages may include requiring in-house expertise to be developed, intensive training programmes, or greater expenditure.

Outsourced development

Advantages may include the IT function's better ability to focus on the core tax administration activities, access to new technologies, reduced ongoing expenditure, and greater flexibility. Disadvantages may include the need to control third party providers and their employees, potential cultural disagreement as between the provider and in-house personnel, or confidentiality concerns.

Information Security Management framework that adheres to internationally recognised standards or best practices (Core Requirement 3.2)

FIGURE 12. **Types of security controls**


Security controls available (technical, administrative, physical)
Tax administration's risk assessment
Tax administration's minimal security requirements
Determines
Tax administration's specific risks
Identifies
Tax administration's residual risks
Selects
Selects
Selects
Baseline security controls
Additional security controls
Enhanced security controls

- **Additional controls**: Additional measures deployed to mitigate identified risks, based on the risks' assessed severity level. As discussed in SR 3.2.1.4, while identifying their risks, tax administrations will have to decide, for each risk, the way they want to handle it, including the controls to apply. Controls would therefore be applied depending on a tax administration's risk appetite.

- **Enhanced controls**: Controls that help deal with advanced threats, such as technologies to detect and prevent data exfiltration (i.e. unauthorised transfer of data).

Tax administrations are expected to assess the effectiveness of the security controls applied, preferably with the use of metrics, and have a formal process for these reviews.

Each type of control can be, in nature, administrative (e.g. a policy or process), physical (e.g. surveillance cameras) or technical (e.g. a firewall or a software). A combination of these different controls may be required to mitigate a single risk (see examples in Table 16). The different types of controls are discussed in turn.

Baseline controls

Depending on the sensitivity of the information hosted on a system, and the level of confidentiality required, commensurate baseline controls will be chosen.

Table 16. **Examples of baseline, additional, and enhanced controls**

Baseline controls	Antivirus, logging & monitoring	CCTV, light system	Password policy
Additional controls	Multi-factor authentication	Fences, mantraps	Awareness training policy
Enhanced controls	Data Loss Prevention systems, continuous in-house Security Operations Centre	Tier 1 data centre, hot site active/active replication	"Bring your own device" policy, enhanced encryption policy for highly sensitive information

Box 23. **Baseline control examples**

Antivirus and firewalls

Antivirus and firewalls are mandatory protections. While the need for these two controls is deemed obvious by most organisations, numerous cyber-attacks take advantage of bad configuration and improper management of those equipment and software.

While antivirus protects workstations and servers against known threats, firewalls help isolate different parts of the network and raise alerts when improper traffic is detected. Maintaining antivirus up to date and properly configuring firewall rules are essential requirements.

Patch and update management

Patching applications and operating systems is a critical aspect of protecting the IT infrastructure. Often, cyber threats such as hacking involve using published exploit code that targets a vulnerability for which a patch has already existed for a considerable amount of time. Hackers are aware that while externally facing systems are routinely patched, internal ones may, for business reasons, not be patched as rigorously.

Patches should be installed by default. Issues with patches can occur, but they are generally rare, and in the event of an issue they can be rolled back until the issue has been incorporated into the next version of the patch.

Tax administrations are encouraged to draft and enforce a patch management policy as a control that ensures patches and updates to all operating systems and firmware are deployed within a defined timeframe (usually within days). A critical patch deployment process should be also in place to ensure that critical patches are deployed within defined timeframes (usually within hours). Tax administrations might also define how they would classify a patch as critical.

System hardening

Configuring systems to be secure by default is a necessary protection against cyber threats. Tax administrations should be able to stop hackers executing malicious code within their IT environment, and it is important to be aware of what is running within the environment to be sure that it is appropriate.

To achieve this, tax administrations should set up standard operating systems as recommended by vendors. Regarding the use of applications, the implementation of a whitelisting tool can be set up to restrict the execution of only authorised executables and scripts. In addition, macros should be restricted so as to require approval to execute, or only if they are signed. Finally, it is important to disable applications that are potentially dangerous, such as web browser add-ons, web advertising, and applets.

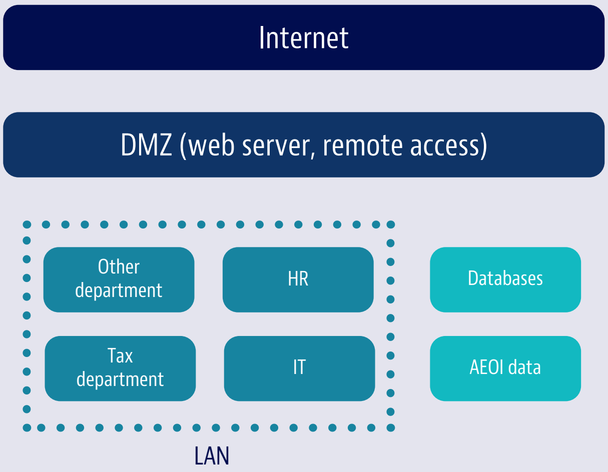
Network segmentation

Implementing network segmentation consists of putting walls up between critical systems and internal and external networks. A 'flat segment', with no or limited such walls, can create an environment that requires only a single network intrusion for a hacker to gain widespread access. A flat network allows the hacker to pivot between hosts and services with minimal obstruction and limited chance of detection. A compromised workstation should not be able to connect to important databases.

A common way to design networks is to cut the network into smaller networks, as illustrated by the figure below, normally having dedicated zones for:

- Externally facing systems, usually called DMZ (De-Militarised Zone).
- A dedicated administrator zone.
- A zone for sensitive databases and critical applications, such as AEOI databases and applications.
- A zone for the internal network, usually called LAN (Local Area Network).

Internal networks can be sub-segmented by activity, e.g. human resources, finance, IT, tax compliance department, etc. The following is an example of network segmentation.



Administrator access and rights management

Hackers target privileged and administrator accounts to carry out their activities, such as extracting data from databases and ex-filtrating data, as these accounts are normally able to bypass any restrictions. It is therefore important to restrict administrator rights and accesses through appropriate management.

It is highly recommended to implement multi-factor authentication (addressed in more detail in SR 3.2.3 about access management) for tax administrations' administrator accounts, to disable or rename all built in system accounts, and to enforce a policy to ensure that administrators' access is restricted wherever possible.

Further, privileged accounts should be prevented from reading emails and accessing the internet generally, including obtaining or uploading files via online services. Also, "jump boxes" can be used as a stepping stone for administrators to access critical systems. A jump box consists of a secured dedicated server located in a DMZ zone, allowing only a few communication protocols in order to allow administrators to authenticate using strong authentication, and then to access specific resources located on the internal network.

Information Security Management framework that adheres to internationally recognised standards or best practices (Core Requirement 3.2)

Box 23 contains examples of common baseline controls based on IT security risks.

Baseline controls are not static: controls that were not very common not long ago may today be considered baseline controls for many tax administrations, for example Security Information and Event Management (SIEM) solutions.

Additional controls

A tax administration may decide to apply additional controls to mitigate identified risks, based on its evaluation of the relative significance or severity of those risks and its risk treatment decisions.

Box 24. **Additional control example: penetration testing of external interfaces**

Penetration testing is a key aspect of understanding whether weaknesses exist in the IT environment. Also known as "ethical hacking", it simulates the actions of a hacker against the organisation. The main purpose is to find exploitable vulnerabilities before anybody else does, so that they can be patched and addressed accordingly. During a penetration test, risks will normally be identified and given a rating against the risk matrix, commonly as follows:

- Low
- Medium/Moderate
- Significant/Serious
- High/Severe/Critical/Catastrophic

The multiple integration points and services that exist in modern IT environments mean that failure to penetration test external and internal interfaces could jeopardise the security of data, including exchanged information (e.g. there may be risks to exchanged information if it has some level of integration with core system environments of the tax administration).

While internal testing is very important, it is particularly important to test external interfaces as hackers anywhere in the world can directly target them. An external interface is simply any service that responds to external input. It could be a value added tax online form, a taxpayer portal, or an file transfer protocol server. Penetration testing is detailed further in SR 3.2.6.4 about vulnerability management.

Additional IT controls complement baseline controls, and will similarly include administrative controls, technical controls and physical controls that together seek to achieve the ultimate goal of confidentiality. This is described as "defense in depth". Box 24 provides an example of a common type of additional control.

Enhanced controls

Enhanced controls can also be used to protect the IT infrastructure against advanced threats, such as sophisticated data ex-filtration methods. Tax administrations deploy enhanced controls as a function

Box 25. **Enhanced control example: Data Loss Prevention (DLP)**

DLP detects potential data breaches including sophisticated data ex-filtration transmissions and prevents them by monitoring, detecting and blocking sensitive data while in use (endpoint actions), in motion (network traffic), and at rest (data storage). DLP detects sensitive data leaving and transiting within the tax administration where it is not supposed to, and takes actions in relation to this data such as blocking, allowing or sending alerts.

A DLP solution is a combination of two DLP tools:

- Endpoints DLP, which consists of software installed on all laptops and workstations that analyses data stored on the equipment, and prevent users from performing prohibited actions, such as copying a file onto an external storage device.
- Network DLP, which prevents data leakage while data is transiting across a tax administration's network, for instance when an email is sent to an external recipient.

To obtain the best results from a DLP solution, it is very important to properly label all data (depending on the tax administration's data classification: see SR 3.2.5.1 about protection of information). DLP systems require highly skilled technicians to be efficient and properly set up.

of the maturity of their existing security processes and controls, and of the overall level of risk in relation to potential data breaches (both in relation to domestic tax data, and exchanged information). See Box 25 for an example of enhanced control.

Assessing the effectiveness of security controls

Tax administrations should take measures to assess the effectiveness of security controls (baseline, additional, and enhanced), as while these may have been implemented they may not work well in practice (e.g. an awareness program is put in place, but after reviewing it the organisation learns that only 5% of the target population effectively followed it). Helpful tools to measure effectiveness include key performance indicators, penetration tests, vulnerability assessments, and data set tests (See SR 3.2.6.4 on vulnerability management for further details).

SR 3.2.4.3. Management of IT assets and services, and service level management

SR 3.2.4.3 is about the operational management of tax administrations' IT assets. Asset management is relevant to the confidentiality of information as assets may contain information, and information on assets is needed to support the investigation of security incidents.

Each IT asset should be identified and managed, as it represents a potential security exposure, and therefore a risk.

Asset management can be divided into two functions, usually performed by separate areas within an IT department:

- **Management of IT assets and services**, usually handled by dedicated IT asset managers.

Table 17. **Asset management lifecycle**

Component of asset management	Description of the component	Examples of items to include	Examples of details to record
Asset inventory	List detailing every single IT asset owned by the tax administration, with its description and a unique identifier	Workstations, hard drives, laptops, screens, mobile devices, routers, firewalls, headsets, software licenses	ID – description - serial number - classification - status to "in use" or "available for use"
Asset ownership	Specification of the asset owner	Entity, person, service, third-party	Owner - function – last review
Asset configuration management	Ensures that systems are properly configured and ready for use	Warranty, software licence management, patch management, deployment, code review	Firmware version – last update – previous owners - status to "configuration in progress" – patch status, warranty status, maintenance status
Asset capacity management	Provides a plan to manage IT capacity, to make sure IT is resourced for use and will be able to grow	Data centre capacity, available equipment for new employees, back-up tape capacity, availability of information	Hardware capacity (%) – last hardware upgrade - remaining storage - electricity consumption - server load - bandwidth
Asset disposal	How the tax administration manages asset disposal	Renewal of laptops, printers, destruction of equipment, sanitisation policy	Status update to "not in use", "sanitise", "sold"

- **Service level management**, or the management of the relationships that underpin the delivery of the IT assets and services to their users in the tax administration. It is usually linked to business relationship managers.

Management of IT assets and services

Table 17 describes the components of asset management that a tax administration would be expected to follow. The components can also be referred to as the lifecycle phases of asset management.

Ideally, all assets should be managed to a similar standard, irrespective of the number of assets held, in order to ensure correct metrics, consistent data, easier monitoring and auditing. Asset management is usually supported by IT tools (see Box 26).

Nonetheless, some variables may influence how tax administrations manage assets:

- **Assets can be managed to different levels of detail**. A desktop PC, for example, can be recorded as a single asset, or it can be documented down to the component level. While either approach is considered valid, the approach has to be sufficiently detailed to be able to identify the relevant attributes of the asset. For example, it is not enough to only record the number of PCs held in a particular office, without information about the PCs' attributes (e.g.: serial number, model, brand, technical information).

- **The management of IT assets can be outsourced**. If a tax administration outsources IT asset management, it must assess and assure itself that the provider is doing the job correctly and effectively. While outsourcing removes a burden for the tax administration, it may require greater effort in monitoring the provider.

A number of tax administration processes may rely on asset information, and tax administrations should be able to support these processes and make changes to services without jeopardising confidentiality. For example, if changes to software will affect assets such as browsers, the tax administration may need to check whether all the different browser types and versions in use in the administration have been tested against the changes. Tax administrations should be able to identify which software versions are in use, on which devices, and that all are running versions that are still supported with security updates.

Service level management

Service level management is about the overarching relationships between the tax business divisions that commission IT services and the entities with overall responsibility for providing the IT services (i.e. the tax administration's IT department, or an external provider).

Those relationships are mainly expressed through a Service Level Agreement (SLA). SLAs encapsulate an agreement between those parties on an IT service's non-functional requirements only. Functional requirements relate to business divisions' objectives (i.e. what an IT application or service should do) whereas non-functional requirements are service based (i.e. the minimum acceptable availability of service).

SLAs are part of supplier agreements, whether the supplier is the IT department (or a sub function of it) itself, or the IT service is outsourced by the IT department.

In addition to SLAs, service level management covers:

- **Operational level agreements**, made between internal entities in a tax administration when the IT service depends on another department to fully operate.

Box 26. **IT tools for asset management**

Ideally, asset management will be carried out using tools such as a Configuration Management DataBase (CMDB), which records all different IT assets including PCs, laptops, peripherals, off-the-shelf software, etc., and is kept up to date in an automated manner. This tool will set out all relevant asset lifecycle information for each asset (e.g. date purchased, version, current location and owner, end of life date, etc.). This information is very useful in a security context because if there is a security incident, an up to date CMDB will enable those investigating the incident to get to the heart of the problem more speedily. Such tool also mitigates risks associated with managing change, and enables the IT department to provide a better service to users.

- **Underpinning contracts**, which are the same as operational level agreements, but where an IT provider relies also on services provided by a sub-contractor.

Service Level Agreements

SLAs in tax administrations ensure that IT services meet the needs of all interested parties within the administration, including directors and other senior managers responsible for the tax processes supported by the IT services, employees who use the systems, and the ISO.

The non-functional requirements in SLAs usually contain:

- **A baseline set of security requirements**, such as managing the provider's (internal or external) access to the tax administration's systems.
- **Specific additional requirements** that may have been identified for a particular system, that supplement the baseline requirements. These may include specifying the manner in which the supplier must handle specific types of data, such as exchanged information or financial data.

Some non-functional requirements will be built into the design of IT services and the infrastructure environment (e.g. firewalls, server hardening or antivirus), whereas others will not be in-built and will need to be monitored by the IT department (e.g. access to data). In both cases, security requirements should be managed effectively for good security outcomes to be achieved. Both need to be addressed in SLAs.

Non functional requirements in SLAs that do not directly relate to security should include:

- A description of the service, including key outputs and deliverables.
- Service availability and other performance targets.
- Maintenance arrangements.
- Rules for planned downtime, including periods for which downtime must be avoided.
- Recovery times.
- Rules for dealing with system change.
- Arrangements for the reporting of incidents.
- Contact points.

The main points to consider when implementing SLA are:

- The overall arrangements, in particular whether there is a single set of standard requirements versus separate supplementary requirements for each system.
- The nature of the agreements, that is, whether it will be a straightforward SLA between the tax business areas and the in-house IT department, or something more complex involving external providers.
- The reporting arrangements, both written and via regular stakeholder meetings (both to be set out in the SLA).
- Whether there is a standardised set of security requirements, e.g. two or more standard sets for different types of processes, or different arrangements for each different system.
- Whether the systems that handle exchanged information, e.g. under the AEOI standard, have their own separate SLA. If not, whether there is any process within the umbrella of an overarching SLA that enables the relevant EOI team to validate that all the relevant security controls are in place and working, in co-operation with the relevant provider (in-house or external) of the IT services.
- The actions needed in exceptional circumstances, particularly incident reporting. Notably, where the IT department identifies a security incident, it should be reported in the prescribed manner.
- The nomination of contact points both within the IT department and across the wider tax administration.

Box 27 shows a basic SLA template.

One noteworthy point to consider is the use of one or multiple SLAs. Some administrations may take a central decision that all IT applications should be built, possibly on a single infrastructure platform with a unique SLA, while others may agree separate SLAs for each of the different tax management applications.

In practice, tax administrations use a mixture of the two. Typically, a tax administration will have reached the point of having a range of different legacy platforms. Managing IT can be complex under these circumstances, so tax administrations may therefore wish to consider standardising IT services onto a single, modern platform. New applications may then be built onto that platform, and legacy applications will migrate as and when circumstances permit. Every few years a new IT paradigm emerges, and the process starts all over again.

Many different factors will need to be considered when deciding which SLA structure is most appropriate for an organisation to use.

In any case, multi-level SLAs are most commonly used, and their level components include:

Organisation level

This level deals with all general issues relevant to the organisation, and that are the same throughout the entire organisation. For example, under the security conditions of an SLA at the organisation level, every employee may be required to create a password of 8 characters and must change it every thirty days; or every employee may be required to have an access card with an imprinted photograph.

Customer level

This level deals with those issues specific to a user or 'client' of the IT service. For example, the security requirements of one or more departments within the organisation may be higher than in other departments, e.g. a financial division or EOI division that requires enhanced security measures by virtue of its role handling particularly sensitive information and resources.

Service level

This level deals with the issues relevant to a specific service (in relation to the user or client). It applies to all users or clients that benefit from the same service — for example, contracting IT support services for everyone who uses a particular IP telephony provider.

Box 27. **Basic template of what to expect in a SLA document**

A SLA typically consists of:

- An introduction, outlining the purpose of the agreement.
- A service description, outlining what service(s) the SLA supports and details of the service(s).
- Mutual responsibilities, i.e. who is responsible for what part of the service(s).
- An outline of the SLA's scope.
- Applicable service hours, i.e. from what times until what times the service(s) is available according to the agreement.
- Service availability, i.e. the extent to which the service(s) is available during the service window and outside of the service window.
- Reliability of service.
- Customer support arrangements.
- Contact points and escalation, including a communication matrix.
- Service performance indicators.
- Security requirements.
- Costs and charging method used.

Using such a multi-level SLA structure for a large organisation may reduce the duplication of effort while still providing customisation for different user and services within the organisation.

Table 18 provides an example of user or client support arrangements that a service provider may guarantee under an SLA, depending on the severity or urgency of an issue. As shown, the greater the severity or urgency, the shorter the response time. In this example, assurance is provided for 90% of reported incidents or issues, meaning that at the end of the relevant agreed service period, a calculation will be made of the issues on which a response was provided. If the score is less than 90% for resolution on time, financial penalties or other compensation could be sought from the supplier. Therefore, both the service provider and the recipient should monitor and compare the figures.

Table 18. **Example of user or client support arrangements under an SLA**

Priority/ Description	Low	Normal	High	Critical
Incident severity	No obstacle to the tax administration's work.	Interruption to the tax administration's work; work-around likely available.	Interruption to critical processes affecting individual users; no workaround available.	Interruption to critical tax administration's processes affecting several users; no work-around available.
Remediation urgency	Tax administration does not need immediate remediation.	Tax administration does not need immediate remediation.	Tax administration needs immediate remediation.	Tax administration needs immediate remediation.
SLA targets				
90% first response time	Within 2 days	Same business day	Within 4 hours	Within 2 hours
90% resolution time	Within 2 weeks	Within 1 week	2-3 working days	24 hours (immediate hotfix)

SR 3.2.4.4. Management of supplier service delivery

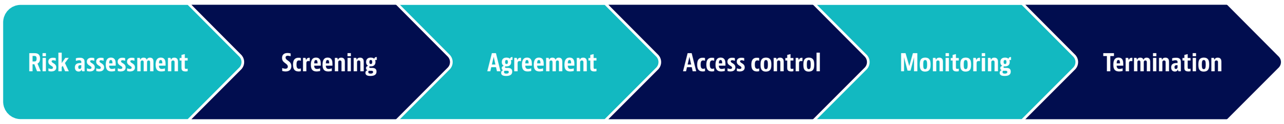
SR 3.2.4.4 is about ensuring security in the use of outsourcing and supply chains by carefully managing a tax administration's relationships with suppliers. This is a very important requirement, as there have been several high profile security breaches traced back to deficiencies in the supplier network.

Many tax administrations seek to ensure that all taxpayer data remains on premises at all times, operated and controlled by them and/or other government agencies with tight oversight over any third party access. Nevertheless, tax administrations are increasingly allowing third party IT suppliers to access their data centres remotely in order to provide remote development, maintenance and upgrade support. In those cases, the types of access permitted should be clearly established and appropriate controls should be in place. A supplier management process is summarised on Figure 13.

A tax administration's contractual agreements with suppliers should include specific requirements to address information security risks associated with IT services and the product supply chain. As an example, in relation to a cloud-based email system or human resources application from a supplier, the agreement should ensure (see Box 28) that the provider also complies with all applicable security requirements and safeguards, especially when processing data and information.

In light of the need to address the information security risks in the context of using suppliers, tax administrations should generally define an information security policy to protect the assets and data that are accessible by suppliers. This policy

FIGURE 13. **Supplier management process**



should be agreed with suppliers and documented. By implication, the specific risks should be identified, and will need security controls applied, as described in SR 3.2.4.2 on deploying an appropriate range of security controls. Some controls may be implemented by the tax administration itself, whereas others are left for suppliers to implement. Such controls could include:

- Identifying, categorising and documenting all suppliers, and defining the type of information they would be allowed to access.
- Awareness training on confidentiality for the tax administration's personnel with regard to the information they handle in conjunction with suppliers and how they should interact with suppliers.
- SLAs.
- Non-Disclosure Agreements.
- Incident handling procedures and processes.

Box 28. **Security in supplier agreements**

It is highly recommended that tax administrations formally agree security requirements with each supplier that may access, process, store, communicate or provide IT components or services and/or access their data. The following items are commonly documented in supplier agreements:

- A description of the information provided to or accessed by the supplier, and the methods of provision or access to the information.
- The classification of the information.
- The legal and regulatory requirements relating to confidentiality and security.
- The obligations of each party to implement relevant security controls, and, where appropriate, to comply with a recognised international standard on information security.
- Rules on acceptable and unacceptable uses of the information.
- If appropriate, a list of the supplier's personnel authorised to access or receive the tax administration's information (or the conditions and procedures to obtain such authorisation).
- The tax administration's information security policies applicable to the agreement.
- The arrangements to deal with situations where the supplier becomes unable to supply its product or service, to avoid any problems and delays in the tax administration's business.
- Conflict resolution processes.

It should be noted that agreements could involve other parties, such as sub-contractors. Also, that agreements may significantly vary between different types of suppliers.

Monitoring and reviewing supplier services

Tax administrations should regularly monitor, review, or otherwise ensure that supplier service delivery is subject to audit to make sure that the confidentiality and information security terms and conditions are being adhered to, and that incidents and problems are managed properly.

It might also be appropriate to have in place a service relationship management process that:

- Monitors service performance levels.
- Requests and reviews service reports to be produced by suppliers.
- Provides for audits of the supplier (by the tax administration itself or an independent auditor).

Box 29. **Non-IT suppliers**

Often, data breaches do not relate to IT suppliers but to suppliers of other services. Breaches have arisen, for example, where cleaning contractors have access to customer human resources systems (in order to update details of cleaners on duty and needing building access) and hackers were able to exploit weaknesses in the supplier's IT systems to gain remote access to the organisation's systems. Therefore, it is also important to have non-IT supplier security controls if these suppliers have access to the infrastructure, remotely or otherwise.

- Reviews supplier audit trails and records of information security events, operational problems, failures, tracing of faults and disruptions related to the service delivered.

- Ensures the supplier maintains a sufficient service capability and the agreed service continuity levels.

Tax administrations are encouraged to retain sufficient overall control and visibility into all security aspects for sensitive or critical information or information processing facilities accessed, processed or managed by a supplier. This could be achieved by putting in place reporting processes for the particular areas of change management, vulnerability management, and security incident reporting and response.

The ultimate responsibility for managing supplier relationships should be assigned to a dedicated individual or service management team, and they should take appropriate action when deficiencies in the service delivery are observed.

SR 3.2.4.5. Assuring the continuity of IT services based on Service Level Agreements

As explained in SR 3.2.1, information security is not only about preventing unauthorised access to information, but also ensuring that legitimate users who need access can get it when they need it ("availability" in the "confidentiality, integrity and availability" trichotomy). If personnel cannot trust formal information access services to work properly when they need to access the information to do their job, they might seek to create their own informal access routes, such as downloading subsets of a database onto their own private file-stores.

Insufficient availability therefore leads to unsafe practices and informal access routes, and these in turn pose uncontrolled security risks. Therefore it is important to make sure that the continuity of business services, including IT, is as effective as it can reasonably be.

This section is about ensuring good practice Information Technology Service Continuity (ITSC), with a focus on three key aspects:

- Recovery and resilience.

- Backup of data.

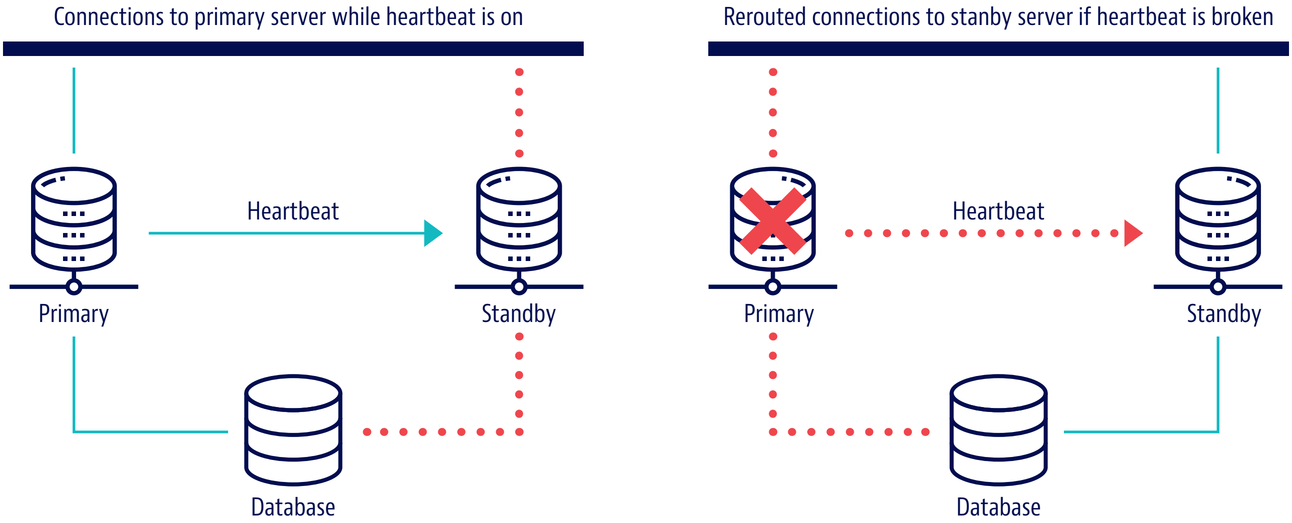
- Plan, implement and verify information security continuity.

Recovery and resilience

Resilience is about mitigating the risk of service interruption, whereas recovery is about restoring a service that has been interrupted.

Any ITSC approach will include elements of both. Moreover, many individual security controls will include elements of both recovery and resilience (see Figure 14 for an example on implementing recovery and resilience through a failover agreement).

FIGURE 14. **Example of a failover agreement**


Connections to primary server while heartbeat is on
Heartbeat
Primary
Standby
Database
Rerouted connections to stanby server if heartbeat is broken
Heartbeat
Primary
Standby
Database

Note: In this case there is a primary (active) server and a secondary (passive) server (so no load balancing). The active server emits a regular "heartbeat" to the standby server, and the failover is triggered if the heartbeat fails.

Resilience has the advantage that it is more effective in reducing the instances of service interruption. Based on recognised international good practices, the steps that a tax administration can take to improve resilience, and therefore availability of service, include:

- Ensuring resilience at the component and service levels. When services are being built or changed, it is important to make sure that the service elements and the components that support service elements are selected, designed, built and maintained in a way that enhances resilience and reduces the risk of service interruption.

- Ensuring multiple instances of the same service. Having two parallel instances of the same service means that if there is a component failure in one of the instances, then processing is switched to the remaining operable instance.

- Ensuring backup power supply. At the data centre level, there are single points of failure, such as water supply, air conditioning and power. Where possible, there should be a backup power supply, either drawn from a separate grid or some sort of Uninterrupted Power Supply (UPS) backup. The assurance of availability in data centres is called "Tier level". There are 4 tier levels and the choice should be made based on the unavailability time that a tax administration is willing to accept. This classification is provided by The Uptime Institute, founded in 1993.

    - A **Tier 1** data centre has a single path for power and cooling and few, if any, redundant and backup components. It has an expected uptime of 99.671% (28.8 hours of downtime annually).

    - A **Tier 2** data centre has a single path for power and cooling and some redundant and backup components. It has an expected uptime of 99.741% (22 hours of downtime annually).

    - A **Tier 3** data centre has multiple paths for power and cooling and systems in place to update and maintain it without taking it offline. It has an expected uptime of 99.982% (1.6 hours of downtime annually).

    - A **Tier 4** data centre is built to be completely fault tolerant and has redundancy for every component. It has an expected uptime of 99.995% (26.3 minutes of downtime annually).

- Ensuring operating services from multiple data centres. Smaller and medium size jurisdictions should consider having some sort of backup facility where at least some processing is carried on day in and day out, even if it is not sized to the same level as the principal data centre. The largest administrations will in any event operate from multiple data centres, and it is desirable to design centres so that processing can change seamlessly between centres. One option here is a backup data centre that is not actively used, but which can be used in the event of an emergency. The advantage of such an arrangement is that the backup can be shared with other organisations so that the cost is more manageable. The disadvantage of such arrangements is that it only works if other organisations don't need the backup at the same time, as might happen in the case of an environmental disaster.

- Using a dedicated site to restart business operations in case of high failure. A tax administration, depending on its costs and needs, might choose a cold, warm, hot or mobile site solution:

    - A **cold site** provides facilities, air conditioning, power, racks and cabling.

    - A **warm site** provides cold site features plus dedicated hardware and software similar to a tax administration's infrastructure, but no data.

    - A **hot site** is a real-time replication of tax administration's data centre, containing exactly the same equipment and data.

    - A **mobile site** is similar to a hot site but in military mobile racks, so is easily transportable.

A tax administration may also choose to replicate only a part of its business services, or those that are most critical or contain the most sensitive data (e.g. taxpayer data, or exchanged data).

Backup of data

A tax administration's data should be backed up. For jurisdictions with multiple data centres connected by dark fibre this may be achieved automatically, with a full back up available at each centre. Generally speaking, however, in most cases some sort of offline back up using tapes and/or disks will be involved. It is important to take into consideration various aspects:

- How the backup is processed.
- Who is responsible for the operation.
- How the offline copies are stored.
- What controls there are to ensure that the downloaded data is not misused.
- The process for testing that a downloaded copy can be restored reliably and accurately.
- How often such tests occur.

In relation to AEOI data, there should be a clear understanding of how data is managed in these processes and how its protection is ensured.

Finally, as the key concerns are availability and confidentiality, it is recommended that highly sensitive data stored (at rest) either this is the actual data or backup, are encrypted with an internationally recognised encryption mechanism (see SR 3.2.5 about protection of information).

Plan, implement and verify information security continuity

An important point to ITSC, as is often the case in IT security, is planning. All aspects covered previously should generally be addressed within BCPs,[16] or Disaster Recovery Plans (DRP), or both. In other words, ITSC should be planned before and after an incident occurs, so security can be continuously managed.

In the absence of business continuity or disaster recovery planning, tax administrations should assume that information security requirements remain the same in adverse situations, compared to normal operational conditions. Alternatively, tax administrations may conduct Business Impact Analyses (BIA) for information security aspects to determine the information security requirements applicable to adverse situations.

For smaller jurisdictions, it is advisable to make planning efforts during the initial business continuity and/or disaster recovery BIAs.

During the implementation of BCP/DRPs, tax administrations are encouraged to establish, document and maintain controls to ensure the required level of continuity for IT services and security. Important aspects to take into consideration include:

- Having an adequate management structure to prepare for, mitigate and respond to a disruptive event. A common example is the definition of a crisis management body involving relevant functions and people.
- Establishing compensating controls against information security controls that cannot be maintained during an adverse situation. For instance, if a power failure occurs, then physical access control might be done manually by security staff while turnstiles might not be working.
- Documenting plans, response and recovery procedures as approved by management.

Once implemented, these controls need to be verified, reviewed and evaluated at regular intervals in order to ensure that they are valid and effective. To achieve this goal, tax administrations may:

- Exercise and test personnel knowledge and the routine to operate IT continuity procedures, processes and controls to ensure their performance is consistent with defined objectives.
- Review the validity and effectiveness of continuity measures when systems, processes, procedures and controls or business continuity/disaster recovery solutions change.

Failure to perform such tests could lead to the full operational failure of systems. An example of this is the lack of data backup testing and restoring, which can lead to full loss of data. This is not an acceptable outcome, in particular, if AEOI data is concerned.

[16] BCM is addressed in detail in SR 3.2.1.5

SUB-REQUIREMENT 3.2.5: PROTECTION OF INFORMATION

"Protection of information" is about protecting the different types of paper and digital information handled by tax administrations, whether at rest, in use, or moving between work environments and locations, with controls commensurate to its sensitivity and confidentiality classification.

SR 3.2.5.1 requires that tax administrations effectively manage information in accordance with a set of policies and procedures throughout the information management lifecycle (including document naming, classification, handling, storage, monitoring, audit, and destruction; and including devices and media that hold information).

More specifically, controls along the information lifecycle include work environment controls such as:

- Clean/clear desk policies.
- Printer controls.
- Physical and digital storage mechanisms for information.
- Encryption and domain controls.
- Secure media controls for information carriers, such as peripheral devices.
- End-of-lifecycle controls, such as information disposal policies.

The protection of *exchanged* information is the specific concern of the Global Forum's assessment process. Tax administrations are therefore expected to ensure that the general controls in place enable that protection, and that appropriate enhanced controls are used to protect exchanged information in particular. The latter are dealt with in SR 3.2.5.2, which requires that tax administrations have processes in place for information received from other competent authorities to ensure that obligations under international exchange agreements are met, including to prevent comingling with other information.

It is important to differentiate SR 3.2.5 from other SRs, such as those that require controls for logical access to data (SRs 3.2.3.3, 3.2.3.4), for IT system security (SR 3.2.4) and for operational security management (SR 3.2.6). Those SRs describe controls that are applied *generally* to protect information, whereas information lifecycle controls under SR 3.2.5 refer to security controls that should be applied *to data itself* as consequence of confidentiality classification policies.

Table 19. **Glossary of main concepts**

Concept	Description
Acceptable use policy	Set of rules that establish the permitted and prohibited practices in relation to information systems that contain confidential information.
Classification of information	Process of identifying the types of information tax administrations hold and determining the level of protection they should receive.
Clean/clear desk policy	A clean/clear desk policy (CDP) specifies how employees should leave their working space when they leave their desks or the office, to ensure the confidentiality of information.
Competent authority	Competent authority(ies) is/are the person(s) or government authority(ies) designated by a jurisdiction as being competent to exchange information pursuant to any international exchange agreement.
Encryption	Encryption is a protection mechanism applied to data making it accessible only if the proper decryption key is provided.
Media sanitisation	Sanitisation is the process of treating data held on storage media to reduce the likelihood of retrieval and reconstruction to an acceptable level
Retention period	Statutory requirement to retain information for a fixed period even if the information is no longer need for tax business purposes.

This section is divided into three parts:

- A brief outline of the three stages of the information lifecycle in tax administrations.
- A description of the general security controls to be applied at each of those three stages (SR 3.2.5.1).
- An outline of the information lifecycle controls relevant to exchanged information (SR 3.2.5.2).

Table 19 provides definitions of the main concepts covered in SR 3.2.5.

Lifecycle of information

As illustrated in Figure 15, controls for information, whether digital or in paper, need to be applied at the three general stages of the information management lifecycle. Enhanced controls along the lifecycle should apply to exchanged information.

The lifecycle stages and controls are presented based on the usual practice of tax administrations. However, tax administrations are encouraged to adopt a lifecycle approach that works best for them.

Before detailing the controls for the protection of information at each lifecycle stage, it is important to highlight the significance of governance and business processes for the protection of information, as illustrated in Box 30.

SR 3.2.5.1. General information lifecycle controls

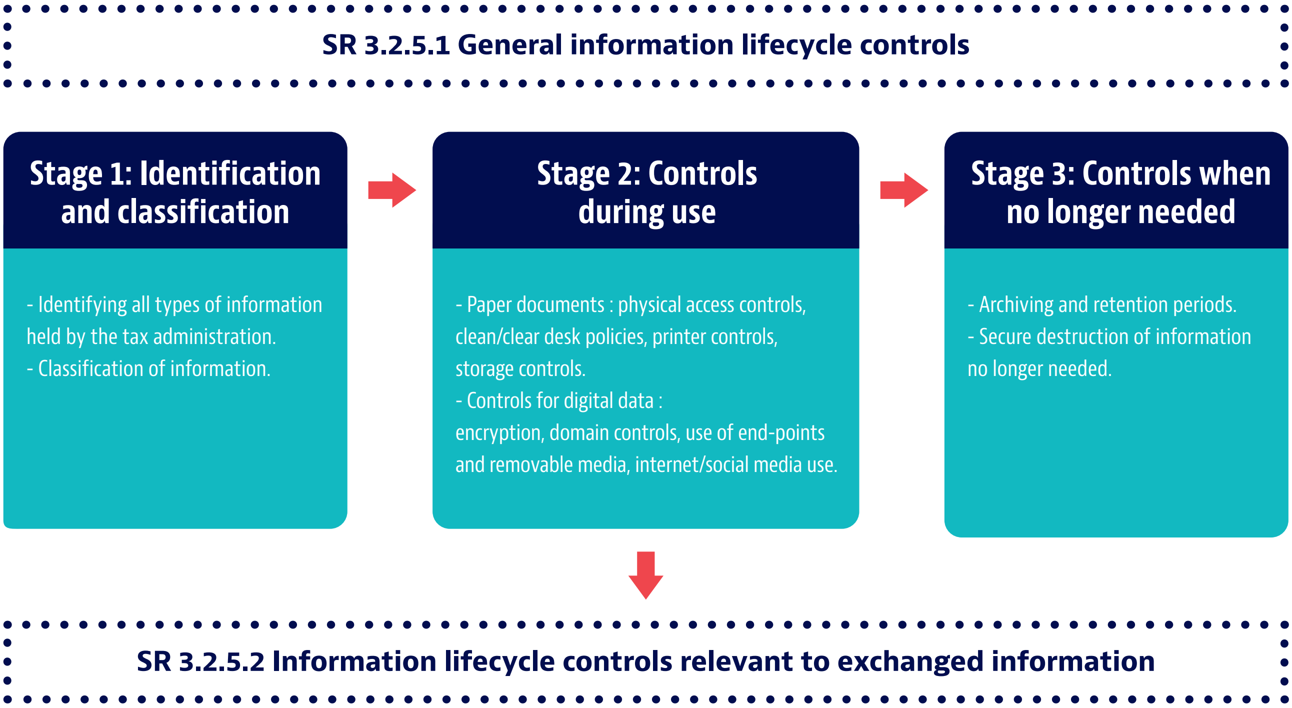
Stage 1. Identification and classification of information

Classification of information is the starting point and the beating heart of information lifecycle management, from where subsequent security controls should flow. The purpose of classifying information is to ensure that it receives protection that is appropriate and proportionate to its classification.

Information handled by tax administrations comes from numerous sources, such as:

- Taxpayer returns.
- Third party reporting from persons with which a taxpayer has a business or employment relationship (e.g. banks, employers).

FIGURE 15. **Information management lifecycle**



SR 3.2.5.1 General information lifecycle controls

Stage 1: Identification and classification

- Identifying all types of information held by the tax administration.
- Classification of information.

Stage 2: Controls during use

- Paper documents : physical access controls, clean/clear desk policies, printer controls, storage controls.
- Controls for digital data : encryption, domain controls, use of end-points and removable media, internet/social media use.

Stage 3: Controls when no longer needed

- Archiving and retention periods.
- Secure destruction of information no longer needed.

SR 3.2.5.2 Information lifecycle controls relevant to exchanged information

Information Security Management framework that adheres to internationally recognised standards or best practices (Core Requirement 3.2)

Box 30. Protection of information, and governance and business processes

Information can only be protected across the lifecycle if it is properly managed with clear governance rules. Ideally, there should be clear lines of accountability for all information assets, each information type having a designated information owner.

In addition, tax information should be managed and handled by users according to well developed and defined business processes. For example, sensitive taxpayer data are usually handled within pre-defined, core tax business processes such as collection and debt recovery. Wherever possible, business processes should be developed for all significant ways in which sensitive data, including exchanged information, are used. This is important because:

- It enables the tax administration to manage effectively, through well-defined policies and procedures, the way in which users access and use data, better protecting it from unauthorised access and misuse.
- Where there are defined processes, it is much easier to evaluate the effectiveness of the process in protecting the data, and to identify and make improvements that make that protection more effective.
- If there is a lack of defined business processes, the likelihood is that there will be no consistency in practice and risky methods of data handling may emerge.

- Reporting from other government agencies, e.g. social security department.
- International EOI.

All these types of information have a certain level of sensitivity and confidentiality, and need to be classified accordingly so that greater levels of protection are applied to the most sensitive information.

If information is not classified or if it is not classified according to its confidentiality and sensitivity level, then two unwanted scenarios could occur: everything is protected to the same high level or everything is protected inadequately.

Protecting all types of information to the same high standards would be too costly and could impair information availability, whereas protecting everything to a lesser standard would expose sensitive information to misuse and to the threat of security breaches by those who should not have access to the information.

Identifying all types of information held

Prior to classification, tax administrations must first know and clearly identify the types of information they are holding. Key information assets held by tax administrations, whether in digital or physical format, usually include:

- Individual and corporate tax returns.
- Information from employers.
- Correspondence with taxpayers.
- Exchanged information (automatic, spontaneous and on request).
- Tax assessments, rulings and determinations.
- Guidance for staff (and guidance for taxpayers) on the completion of tax returns.
- Guidance on the conduct of tax audits and other compliance activities.
- Information in relation to ongoing criminal investigations.
- Internal memoranda, position papers, and research.
- IT information that could be used to gain access to the business information, such as:
    - Access credentials, including system passwords.
    - Source code.
    - Configuration of the gateway and domain appliances.

Classifying the information

Once tax administrations have identified all the types of information they hold, they should classify them, setting out how each category is to be managed and controlled, and clearly reflect this into a policy.

Tax administrations can use different criteria for classification. Generally, four approaches are used, none of which are exclusive of each other (see Table 20). Tax administrations may use more or less criteria, depending on the information they hold, their domestic laws and practices, and the size and scale of their operations.

Each type of information must have its own classification according the criteria used. Table 21 shows a simplified example of a classification of information matrix, noting that the examples provided are not exhaustive and are for reference and illustration purposes only. However, it is important to note that exchanged information should be at least classified as confidential within the tax administration to ensure appropriate controls.

Stage 2. Controls for the protection of information during use

Once tax administrations have defined the types of information they hold and the criteria for their classification, they should then identify the main controls that are appropriate for each category, and clearly translate this into a policy. The control framework devised should enable sensitive and confidential information to be suitably protected while at the same time ensuring that less sensitive information is more readily accessible.

Table 20. **Criteria for the classification of information**

Criteria	Description
Sensitivity	The most common criterion is classification based on sensitivity, with categories that can include: ● Public (e.g. material useable on external website). ● Internal (general office internal communications). ● Restricted/confidential (a category that usually includes taxpayer information). ● Secret/top secret (usually restricted to situations where there is a significant threat to individual or collective interests, e.g. to life, business or commercial interests, or to the workings of the state).
Restricted access	Usually used in conjunction with the sensitivity criterion, this criterion refers to additional controls that are based on the 'need to know' principle rather than sensitivity per se. For example, because of its sensitivity, EOI data are ordinarily categorised as restricted/confidential (it is taxpayer data) but, because of the treaty obligations, access is further restricted on a need to know basis only to those employees that need to handle EOI data to perform their specific duties.
Scale/volume	Large-scale records represent a greater vulnerability than one record, and enhanced controls should be applied where aggregated records are involved. These criteria can be categorised using 'impact levels', which refers to the impact to the confidentiality and integrity of the data if access is compromised, and the type of access controls required according to the impact level. For example, using the scale from 1 to 5, being 1 the lowest impact level and 5 reserved for the highest impact in terms of "threat to life or the state". A single EOI individual record held on a laptop or an encrypted USB stick might be impact level 2 or 3; the AEOI database might be impact level 4. Those categorisations would then determine, for example, the type of access controls required, e.g. whether or not the data should be encrypted.
Information type	This criterion can be used to categorise different types of information, for example human resources or procurement records can be classified as In Confidence, and guidance material for taxpayers can be classified as Not in Confidence.

Information Security Management framework that adheres to internationally recognised standards or best practices (Core Requirement 3.2)

Table 21. **Example of information classification matrix**

Category	1 – Public	2 – Internal use	3 – Confidential	4 – Highly confidential
Description	Information that can be made available to the public and internal information of which unauthorised disclosure would not cause damage to the tax administration.	Internal information of not sensitive nature, but of which unauthorised disclosure could be inappropriate/ inconvenient for the tax administration.	Internal, sensitive information that can only be accessed on a need to know basis, and of which unauthorised disclosure could cause some damage to the tax administration and stakeholders affected.	Internal, highly sensitive, and sometimes large-scale information that can only be accessed by a limited number of persons on a strict need to know basis, and of which unauthorised disclosure could cause serious and/ or extensive damage to the tax administration, and to stakeholders affected.
Information under the category	● Guidance for taxpayers on the completion of tax returns. ● External website.	● Operating procedures for the conduct of tax audits. ● Training materials for staff. ● Non-confidential internal memos.	● Information from employers. ● Correspondence with taxpayer. ● Assessments/ruling/ determinations. ● Contracts, Service Level Agreements. ● Internal confidential memos.	● Individual tax returns. ● EOIR data. ● AEOI data. ● IT information for access to business data (source code, access credentials).

Generally, controls should be applied:

- **While the information is in use or "in motion"**, i.e. being handled for tax business purposes or moved between location or work environments.
- **While stored or "at rest"** between uses.

The controls should draw on the access principles described in SR 3.2.3 (access management), such as the need-to-know and least privileged access principles. Sensitive information, both in physical and digital format, should only be accessible by those with a legitimate business reason.

In the past, taxpayer information was mostly managed in physical format. Over time, with the advancement of technology and the need to more effectively conduct the business of tax administration whilst protecting information, tax administrations have started to move away from the physical file concept and to hold information digitally. Nowadays, information held by most mature tax administrations is either received digitally, or is digitised on receipt and managed through automated workflows. Tax administrations are at different stages of the transition from paper to digital working, and for confidentiality assessment purposes it is important that both formats for managing information, where applicable, are taken into consideration when determining the controls to be applied.

The following sections provide guidance and key good practice controls ordinarily applied by tax administrations in respect of paper and digital information.

Controls for the protection of paper documents

The main elements of protecting paper documents within tax office areas include arrangements for physical access of employees to paper documents, clear desk policy controls, printer controls, and storage controls when information is not in active use and "at rest".

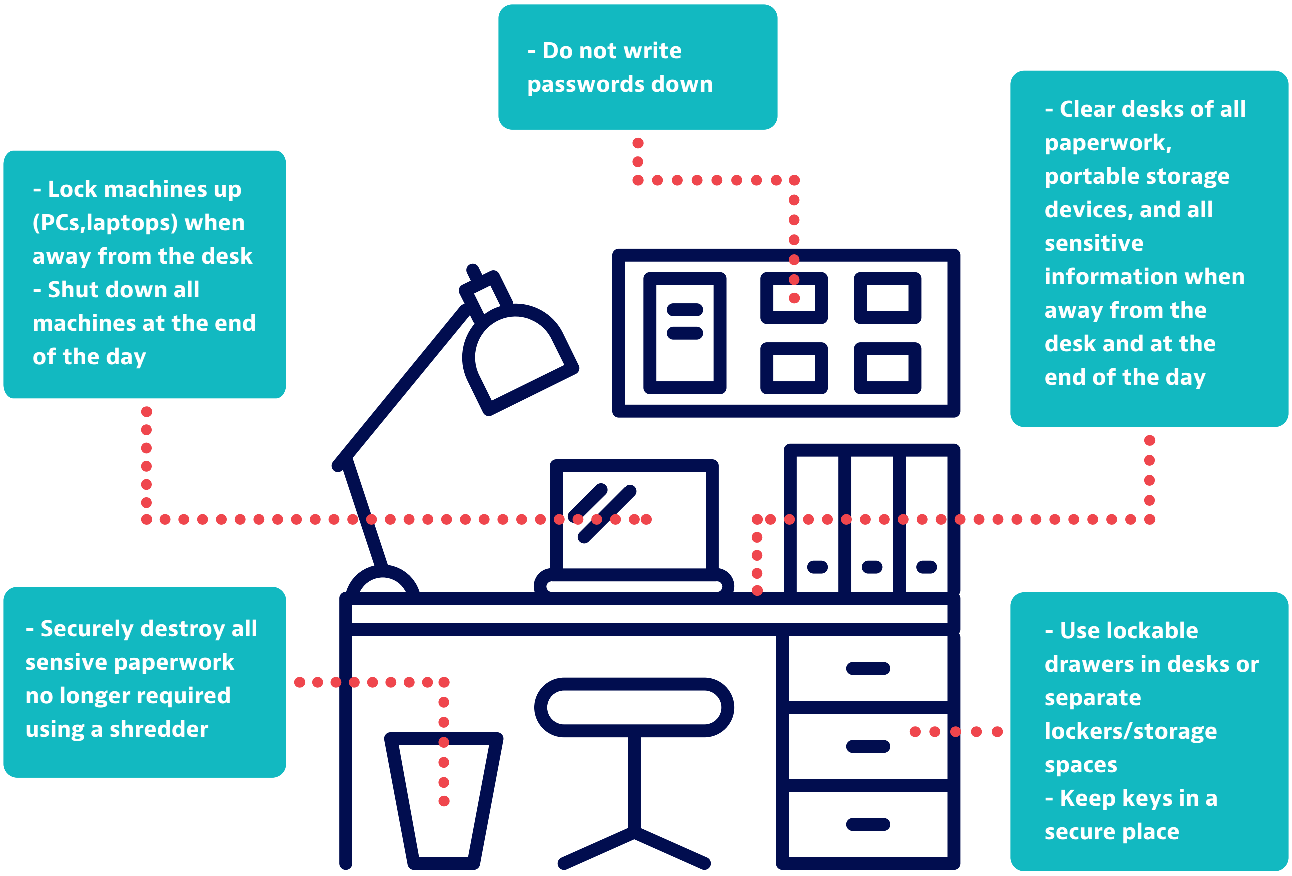
Physical access of authorised personnel to paper documents

Access of employees to paper documents is more difficult to handle in comparison to digital data, as access to the latter can be relatively easier to manage and restrict with logical access controls (see SRs 3.2.3.3 and 3.2.3.4 for controls that govern logical access).

Access to paper documents is usually restricted by:

- Restricting access to buildings and premises to authorised persons only, and implementing controls to segregate workspaces within tax administrations. Security measures can include requiring authorised employees to use an electronic pass, photo-ID, or implementing coded entry systems to enter certain or all office areas, including the EOI unit or other area or file store where sensitive information is located. These controls can be complemented by secondary control systems such as security guards, video surveillance and policies against unaccompanied visitors. These aspects were covered in more detail in the physical security access requirements section, covered in SRs 3.2.3.1 and 3.2.3.2.
- Implementing clear rules regarding the extent of taxpayer information that can be accessed by employees depending on the business need. For example, if an enquiry was made into a particular aspect of a taxpayer's affairs, the tax officer in charge should have access only to the information relevant to that aspect, and not to all of the taxpayer's physical records.
- Labelling documents classified as confidential, and clearly laying out in a policy how the documents labelled or stamped as "confidential" are to be accessed and handled by employees.

FIGURE 16. **Clean/clear desk policy controls**



- Do not write passwords down

- Lock machines up (PCs,laptops) when away from the desk
- Shut down all machines at the end of the day

- Clear desks of all paperwork, portable storage devices, and all sensitive information when away from the desk and at the end of the day

- Securely destroy all sensitive paperwork no longer required using a shredder

- Use lockable drawers in desks or separate lockers/storage spaces
- Keep keys in a secure place

Information Security Management framework that adheres to internationally recognised standards or best practices (Core Requirement 3.2)

Clean/clear desk policy

Controls for physical documentation go beyond managing paper: they are also about good management and control of the desk environment.

A clean/clear desk policy (CDP) specifies how employees should leave their working space when they leave their desks or the office, to enforce the need-to-know principle and prevent non-authorised users from viewing information that is not appropriate for them to see. CDPs limit exposure to employees with no access rights and to external parties (e.g. cleaning staff, repair staff, security guards).

CDPs may require (see Figure 16):

- Employees clearing their desks of all sensitive information, paperwork, portable storage devices (USBs, disc drives) when away from their desks and at the end of the day.
- Locking machines (PCs, laptops) whenever away from the desk or shutting them down at the end of the day.
- Not writing passwords down.
- The use of lockable drawers in desks, or separate lockers or storage spaces.
- Keeping keys in a secure place.
- Secure destruction of all sensitive paperwork no longer required, with the use of shredders.

The office manager or another person responsible might be tasked with checking the office at the end of the day and confiscating or destroying any folders, papers or portable storage media an employee might have left out on their desk.

As with all confidentiality and security policies, to be effective a CDP should be documented and communicated to employees.

Printer controls

Staff may need to print sensitive information held digitally. Once printed, if no adequate controls are in place the effectiveness of logical access controls may be compromised or lost (see SRs 3.2.3.3 and 3.2.3.4 for controls that govern logical access). Printer controls may include:

- Circumstances under which information can and cannot be printed, where possible enforced by coded print rules.
- If sensitive information is printed, establishing clear handling instructions and confidentiality marks, for example, appearing on the printed document as a watermark or header/footer.
- Controls to mitigate the risk that the material is collected from the printer by someone other than the authorised user, e.g. the use of proximity controls so that the intended or authorised user can only complete the printing process by being physically at the machine.
- Sanitisation or encryption of printer storage. As printers have storage, if adequate controls are not taken leased printers could be returned to lessors with the recorded contents of printed material.

Storage controls of paper documents when "at rest"

When paper documents are not in use – meaning that they are stored or "at rest" – tax administrations may consider the following controls:

- Storage of paper documents in locked storage units, safes or rooms. Cabinets or safes should be immobile and locked at all times. Access to keys should be restricted to authorised employees only. The use of multi-lock cabinets for classified and sensitive information is desirable, although if access to premises is sufficiently secure this may compensate for fewer lock controls.
- Use of separate storage areas for taxpayer files and other sensitive documents. The security controls for these areas should ensure access only by employees with a legitimate business need, e.g. security personnel guarding the entrance to the storeroom and permitting access only to authorised staff with photo-ID, security codes to access the storeroom, biometric identification, or video surveillance.
- Inventories of all documents stored.

Box 31 contains an example of controls for paper documents.

The full list of controls to be applied to information can be set out in the form of a matrix or matrices depending on the different classifications of the information, and the scale and the complexity of the information that a tax administration holds. Table 22 shows a simplified example of a matrix with controls for paper documents according to their classification and confidentiality level.

This matrix is for illustrative purposes only and shows examples of controls following the sequence in which they are presented in this toolkit. Tax administrations are encouraged to design matrices that adapt to their own criteria for the classification of information and particular organisational procedures.

Controls for the protection of digital information

When in use, data held digitally may be emailed between staff or travelling across information systems or across

Table 22. **Example of matrix with controls for paper information according to confidentiality level**

1 – Public	2 – Internal use	3 – Confidential	4 – Highly confidential
● No labelling required.	● Labelled as "internal use only".	● Labelled as "confidential".	● Labelled as "highly confidential".
● No restriction on access and no specific storage required. Can be left in unlocked drawers or cabinets.	● Access restricted to specific groups or departments. ● Secured in locked drawers or cabinets.	● Access restricted to specific individuals on a need-to-know basis. ● Must be stored in locked cabinets in desks, or in a room accessible by authorised personnel only.	● Access restricted to specific individuals on a need-to-know basis. ● Secured in unmovable cabinets with high security padlocks, located in a secure room accessible by authorised personnel only. ● Security guards and video surveillance if stored in secure rooms.
● No restriction on copying and printing. ● May be left unsecured at desk or printer.	● Can be copied and printed only by authorised groups and departments ● Cannot be left unsecured at desk or printer.	● Can be copied and printed only by authorised individuals. ● If copied and printed, must not be left unsecured at desk and printer.	● Can be copied and printed only by authorised individuals and with authorisation of a senior manager, on a case-by-case basis. ● If copied and printed, must not be left unsecured at desk and printer. ● All copies must be numbered and recorded.
● Can be disposed of via paper waste.	● Shredding after use.	● Shredding after use.	● Micro or cross-shredding after use.

Box 31. **Example of controls for paper documents**

All confidential information in Jurisdiction A's tax administration, such as taxpayer information, is clearly labelled as "Confidential".

Access to confidential paper information is restricted to specific individuals on a need to know basis and must be stored in locked cabinets in desks, or in a room accessible by authorised personnel only. Confidential information can be copied and printed by authorised individuals only. When away from their desks, hard copies of confidential information have to be securely stowed by personnel in their desk drawers under lock and key. All confidential information must be shredded after use.

All PCs and laptops have to be logged off at the end of the day. The last tax administration officer to leave for the day has to check all desks and switch off all devices that have been left on, and remove any uncollected printouts from the photocopier/printer. Clean desk policies and printer controls are clearly laid out in the Information Security Policy of the administration, and sanctions for non-compliance are applied.

Exchanged information received in paper format is segregated from other taxpayer information received domestically, and records are kept in a secured storeroom which is accessible only to staff in the EOI unit on a need-to-know basis. EOI information must always be returned to the storeroom by the end of the day, and all accesses are logged. Access to the file room is activated with the authorised officer's electronic ID.

jurisdictions (e.g. EOI data). Staff may also use data in removable media. Digital information may also be "at rest", stored in a database within the data centre or saved on a server file system.

Breaches of digital tax data, e.g. AEOI data, could have a massive impact, so it is essential that full consideration is given to the right controls and these, generally, should be risk-based. Specific controls include:

- Encryption.
- Domain controls.
- Controls of endpoints, removable media and peripheral devices.
- Acceptable use policies.
- Computer hardening.
- Controls in relation to internet and social media use.

While these controls overlap with those described in SR 3.2.4.2, SR 3.2.4.2 refers to the main IT system security controls deployed within the IT environment and infrastructure whereas the controls described in this part apply to the data itself.

Encryption

Data is more vulnerable to unauthorised access when in motion and, under international standards, confidential data should be encrypted when in use and when moved from point to point, e.g. between information systems or when being moved by email or through movable media.

While at rest in databases, sensitive data does not necessarily need to be encrypted, provided that other adequate protections are implemented around those databases to ensure that data cannot be compromised. These protections could be implemented through domain controls, addressed in the section immediately below.

When deciding whether to encrypt data at rest, tax administrations may take into account:

- **Risk-analysis**. The approach should be based on risk and a good understanding of the threats.
- **Data performance**. Encryption may affect performance, e.g. delay the presentation of data, and there is a trade-off between confidentiality and availability. However, a tax administration may find that delay acceptable when information is highly sensitive, and it has identified risks to its integrity.

If properly done, encryption can fully protect data. However, even where encryption is used for data at rest, complementary domain controls should be applied to databases, including penetration testing of systems and applications.

Some encryption controls to consider are listed in Box 32:

Box 32. Encryption controls for digital data in transit and at rest

Data in transit

- Controls for transmitting information through web applications (e.g. taxpayer portals), such as Transport Layer Security (TLS) or Hypertext Transfer Protocol Secure (HTTPS).
- Controls for transmitting information during digital exchanges (e.g. video conferences, mobile messaging), such as end-to-end encryption.
- Controls for transmitting information via email, such as StarTLS.

Data at rest

- Controls to prevent breaches of data held in databases, such as symmetric encryption standards.

Domain controls

Like paper information, which is commonly secured by placing it in a single domain such as a safe, digital data is stored in centralised databases with servers that manage access to them. Tax administrations should put in place adequate protections around those databases and servers to ensure that sensitive and confidential data cannot be compromised. These protections are referred to as "domain controls".

While domain controls are dealt with in more detail under SR 3.2.4.2 regarding the IT system security environment as a whole, and in SR 3.2.6 on operational management (logging and audit), they would generally include:

- Segregation of infrastructure environments.
- Firewalls and antivirus.
- Enhanced access controls, such as multi-factor authentication, single-use sign-on, and time-limited access, in particular for privileged accounts.
- Operating system hardening, such as disabling ports.
- Enhanced logging and monitoring.
- Vulnerability scanning and audit.

Hardening of PCs, software maintenance

Protecting digital information also involves controls with respect to PCs and the range of software applications used by personnel, such as PC hardening and software maintenance. As these controls relate not only to the data handled by PCs and software applications but also to the security of the tax administration's IT environment as a whole, they are dealt with in SR 3.2.4.2 about IT security controls.

Endpoints, removable media and peripheral devices

This part refers to controls of end user devices used at the desktop, including:

- Endpoints, e.g. PCs, laptops.
- Removable media, e.g. USB flash drives, external hard drives.
- Peripheral devices, e.g. mouse, keyboard, webcam.

If end user devices have access to sensitive data and are mobile, then controls should be applied. Key controls ordinarily include:

- Encryption of USB sticks.
- Securely sanitising sensitive information that has been transferred to movable media, when the purpose for which it was transferred has been fulfilled.
- Use of dedicated end-point monitoring software.
- Alert systems when unapproved peripherals are used.
- Data loss prevention systems.

Internet, social media and email use

Social hacking is one method used to unlawfully access digital data. Hackers might try to breach data by sending phishing emails to tax administration personnel to distribute malware through tax information networks. Malware could also enter tax administration systems via social networks or platforms.

Although basic phishing emails are often quite crudely constructed and easily spotted by the trained eye, hackers will also use "social engineering" techniques to acquire intelligence about individuals in order to launch carefully crafted email attacks, sometimes referred to as "spear phishing". These will often rely on information about what internal emails look like, and therefore can sometimes be much more difficult to spot. Government email addresses often follow a standardised format, which makes it easier for the more capable hackers to bypass formal controls.

This illustrates that ultimately, humans control the use of IT equipment and it is therefore particularly important that employees have a clear and unambiguous understanding of what is allowed and not allowed in using endpoints, removable media, peripheral devices, internet and social media. The success or failure of managing equipment and services that contains information will be determined primarily by securing the co-operation and support of employees. This is normally achieved by implementing an "acceptable use policy" (AUP).

Although tax administrations may establish AUPs, they may also prefer to wholly avoid risks, e.g. ban the use of removable media, personal emails and social networks or platforms altogether. If an acceptable use policy approach is taken, the reality, however, is that tax administrations only have a certain level of control and influence over employees, so effective training on the risks of using removable media, internet and social media, combined with awareness campaigns, are essential to ensure that the policies are effectively implemented. It is better to train staff to do the right thing, rather than simply relying on disciplinary action when things go wrong.

Some specific elements to include in an AUP are:

- Always assuming an email is a threat unless the employee knows it is genuine, i.e. it is recognised as genuine because it is expected and the sender and email address are known and genuine.
- Never opening attachments unless they are known to be genuine, if necessary checking with the sender before opening.
- Never clicking on links. If a link to an organisation's webpage is demonstrated to be worth pursuing, it is recommended that the employee goes directly to its web site and accesses the link through the home page.

Box 33. Suggested principles for the design of acceptable use policies

Whether an AUP is being designed for the use of removable media or social media, tax administrations may consider:

- **Scope and general rationale**. As a starting point, it is important to stress the general rationale behind the policy, which is the protection of information and taxpayers' rights to privacy. Getting users to understand the function of the policy may facilitate better compliance and co-operation.
- **User rights and responsibilities**. Standard AUPs define the rights and responsibilities of personnel, especially when it comes to ensuring the protection of information.
- **Acceptable uses**. Whenever possible, an AUP should accommodate employees' needs, e.g. internet searches relating to work activities or even handling of urgent personal issues. If non-business use is permitted, the policy should define what non-business use is and specify in what circumstances it is permitted.
- **Prohibited uses**. As an example, internet and social media uses might include specific internet searches, downloads, browsing, and commenting. Most policies include prohibitions against illegal, harmful and offensive use or content, as well as against outright illicit practices such as fraudulent schemes, phishing, abusive or hate-related content, the introduction of viruses, infringement of copyright and intellectual property rights, invasion of privacy, libel and slander, accessing systems without permission, usage exceeding privacy allocations, extracting marketing lists, and sending unsolicited spam.
- **Privacy standards**. This means including provisions on privacy and responsible data use in an AUP. The policy can define what types of data are sensitive and why, and should be specific about the access and use of sensitive data.
- **Sanctions.** The possible consequences and violations following a breach of the policy should be included.

Box 34. **Example of controls applied to digital information**

In Jurisdiction B's tax administration, confidential information held digitally can only be transmitted using encryption. Confidential data, including exchanged information, can only be sent to a tax administration B email domain, or transmitted by authorised individuals to reliable external emails using end-to-end encryption.

Logical access to confidential information is restricted to specific individuals on a need-to-know basis, and access rights of users and administrators are restricted with multi-factor authentication.

All sensitive data are only readable via the tax administration's authorised devices. The acceptable use policy includes a list of all portable storage media devices that are authorised for use within the tax administration. Removable devices containing confidential information must be left in unmovable cabinets or drawers with high security padlocks, or in a room accessible by authorised personnel only. There is a special team within the IT department that carries out regular monitoring of staff's use of endpoints, portable storage media and peripheral devices.

Confidential digital information can be printed only if authorised by senior managers but with the "confidential" watermark, and must not be left unattended once printed.

Confidential information is protected with the use of DLP systems and endpoint protections. Social media use and internet use is blocked within the EOI unit, and specific procedures and sanctions in this regard are laid out in the acceptable use policy.

- Always heeding warnings from anti-virus products and never overriding warnings.
- Always being careful about what employees post onto any social media platform.
- Even if the policy does not permit the use of social media during official business, it may nonetheless be worthwhile highlighting the risks of doing so.
- Only devices approved and issued by the tax administration should be used. These devices should be encrypted as required under the tax administration's data classification policies.
- Devices should only be used as prescribed in tax administration policies.

Box 33 suggests some principles tax administrations may consider for the design of an AUP.

AUPs should be communicated to personnel as part of their on boarding process and under regular staff training and awareness campaigns, as part of the human resources controls in SR 3.2.2.

It is also important that employee activities are monitored, and that managers are involved in the monitoring and enforcement of these policies. There can be two levels of checking:

- Managers should have the responsibility (and should themselves be exemplars) for emphasising the importance of good security, including with respect to using work equipment.
- Security teams in charge should carry out spot checks.

As with paper information, the controls to be applied to digital information can be set out in the form of a matrix or matrices. Table 23 shows a simplified example of a matrix for digital information according to its confidentiality level, and Box 34 gives some examples of controls applied in a tax administration.

Stage 3. Controls when information is no longer needed: retention periods and destruction

This section is concerned with the latter part of the lifecycle, where particular tranches of information need to be disposed of because they become less relevant or cease to be relevant to the needs of tax administration.

A general principle of information security good practice is that information no longer needed should be destroyed. This is because holding information, and in particular holding sensitive information, is inherently risky and as a general rule, the risk is proportional to the sensitivity of the information and the period for which the information is held.

Information Security Management framework that adheres to internationally recognised standards or best practices (Core Requirement 3.2)

Table 23. **Example of matrix with controls for digital information according to confidentiality level**

1 – Public	2 – Internal use	3 – Confidential	4 – Highly confidential
● No encryption. ● Can be emailed between staff, and held in movable device internally.	● No encryption. ● Can be emailed between staff within groups and departments.	● Encryption required on transmission. ● Can only be emailed or transferred using encryption, by authorised individuals.	● Encryption required on transmission. ● Can only be emailed or transferred with encryption, by authorised individuals, and with authorisation of a senior manager on a case-by-case basis.
● No restriction on logical access.	● Logical access restricted to specific groups or departments.	● Logical access restricted to specific individuals on a need to know basis. ● Access rights of users and administrators are restricted with multifactor authentication.	● Logical access restricted to specific individuals on a need to know basis. ● Access rights of users and administrators are restricted with multifactor authentication.
● N/A	● N/A	● Databases segregated from other information. ● Kept on secure servers protected by firewalls, antivirus and passwords.	● Databases segregated from other information. ● Kept on secure servers protected by firewalls, antivirus and passwords.
● Can be held in movable devices. ● Removable media containing this information can be left in unlocked drawers or cabinets.	● Can be held in movable devices within groups and departments. ● Removable media containing this information must be left in locked drawers and cabinets.	● Can only be held in authorised removable devices with encryption. ● Removable devices containing this information must be left in locked cabinets or drawers, or in a room accessible by authorised personnel only.	● Can only be held in authorised removable devices if authorised by senior managers. ● Removable media containing this information must be left in unmovable cabinets with high security padlocks, or in a room accessible by authorised personnel only on a need to know basis. ● Use of endpoint and removable media protection systems. ● Use of DLP systems.
● No restriction on printing.	● Can be printed, but with the "internal use only" watermark, and must not be left unattended once printed.	● Can be printed but with the "confidential" watermark, and must not be left unattended once printed.	● Can be printed only if authorised by senior managers and on a case-by-case basis.

If sensitive information has a useful purpose then the value of retaining the information outweighs the risk of holding it. However, if the information no longer has material value, good practice requires that the sensitive information is destroyed, eliminating any residual risk. It is possible, however, that tax administrations are subject to statutory requirements to retain information for a certain time even if it is no longer needed.

Tax administrations should clearly establish their destruction of information policy, by reference to the applicable retention periods and requirements for the secure disposal of documents, whether physical or digital. The policy should define:

- The different types of documents the tax administration holds.
- Their security classification.
- The reasons for which the documents are retained.
- The duration for which the documents are required to be retained.
- The retention mechanisms.
- The methods and processes for sanitisation or destruction.

The policy should be supported by processes for reviewing documents throughout their lifecycle to make sure that they are still needed and are being used, and procedures for action to be taken at the point when they are no longer needed.

The fact that the information is no longer needed does not necessarily mean, however, that the information has to be automatically destroyed. Policies can provide for a review process before destruction or deletion occurs.

If the decision to continue retaining or to destroy the information is taken, then there should be a register of:

- The information that is being retained or destroyed.
- The business reason for retention or destruction.
- The next review date if the information is further retained.

Decisions on retention or destruction of information should be taken by senior managers or information owners with overall responsibility for that part of the tax administration's operations or type of information.

Retention periods

Although, as a general principle, good practice would require information that is no longer needed to be destroyed, tax administrations may have statutory requirements to retain information for a fixed period even if no longer needed for tax purposes. In some cases, that period is permanent. In other instances, there is a requirement to send subsets of taxpayer information to national archives.

If mandatory retention periods apply, then tax administrations should evaluate the risks of holding the information and take adequate measures to mitigate the risk of retention to an acceptable level. It is important that the information owner takes responsibility for those risks and for ensuring that the mitigation measures are effectively put in place. These mitigating measures can include:

Paper documents

- **Sorting or weeding**. Only keeping papers that are strictly required to be retained.
- **More secure storage**. Papers that are still consulted regularly can be kept in storage facilities designed to make access easier, and documents that are no longer needed may be archived in a more secure repository.
- **Digitising physical documents and storing electronic copy offline**. This applies only if there is no forensic reason for retaining the paper version. In some jurisdictions, the rules of evidence require that the original paper copy is used in legal proceedings rather than a digital copy. Therefore, it is important to establish whether the laws in the particular jurisdiction have this requirement and preserve the original paper copy accordingly.

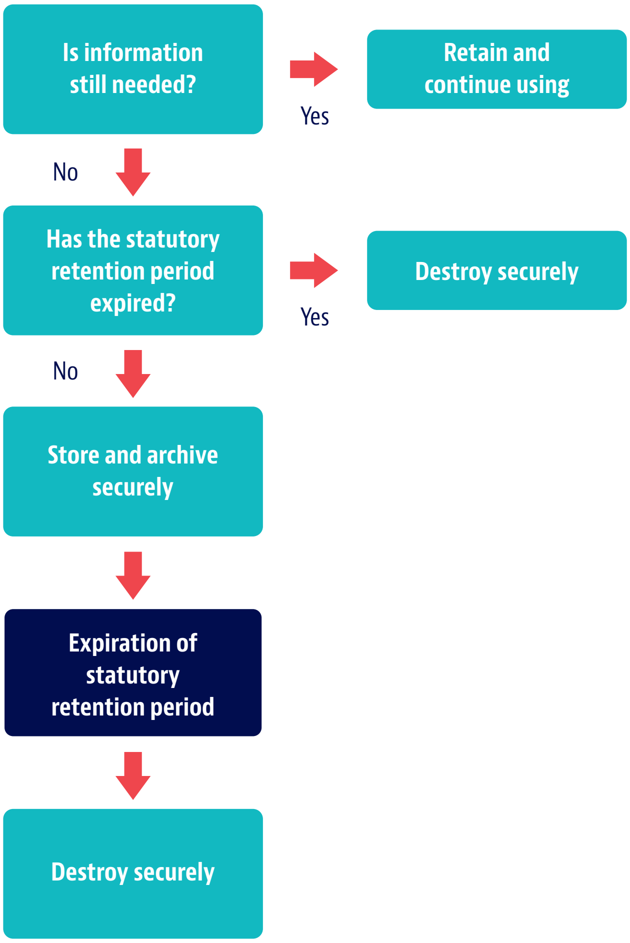
Digital documents:

- **Data encryption**. Encryption can lower the security risk of retaining information.
- **Moving older data sets to offline storage**. Offline

storage means that the storage device is not ordinarily connected to any operating environment, and is only connected as needed. This could either take the form of a separate database, or some form of removable media such as an external drive. It is important that offline storage is stored securely and checked regularly.

Tax administrations should maintain proper records of all material, whether physical or digital, that is being retained. See Figure 17 for an example of a process for retaining and destroying information.

FIGURE 17. **Example of process for retaining and destroying information**


Is information still needed?
Yes
Retain and continue using
No
Has the statutory retention period expired?
Yes
Destroy securely
No
Store and archive securely
Expiration of statutory retention period
Destroy securely

Secure disposal of information

Tax administrations should use methods to securely destroy or sanitise information that are proportionate to its sensitivity. The methods should ensure that no material can be recovered after destruction or sanitisation. There should also be clear procedures to determine the basis on which information, or media that contain information, are identified and selected for sanitisation or destruction.

Box 35. **Sanitisation of storage media and why it is important**

Sanitisation is the process of treating data held on storage media to reduce the likelihood of retrieval and reconstruction to an acceptable level. Some forms of sanitisation will allow tax administrations to re-use the media, while others are destructive in nature and render the media unusable.

When to sanitise media

There are various circumstances in which tax administrations may consider sanitising storage media:

- Re-use: when a device will be allocated to a different user or repurposed within the tax administration.
- Repair: when returning a faulty device to the vendor for repair or replacement.
- Disposal or destruction: sanitising unwanted media before it is disposed of or destroyed, especially if a third party has been contracted by the tax administration to dispose or destroy of the material.

In all cases, the media will be outside its normal operating environment and with a different set of users (e.g. third parties and or less trusted organisations and individuals), and is therefore subject to greater risk.

The risks of not sanitising

If storage media is not properly sanitised, sensitive data may remain, opening risks of:

- Unknown whereabouts of sensitive data of loss of control over information assets.
- Confidential taxpayer data being recovered and used to commit fraud or identity theft.

Source: www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media

In case of information held by third parties or external contractors, tax administrations should also establish destruction or disposal requirements and these would be laid out in the contracts or SLAs.

Methods for destroying or sanitising information include:

Paper

Normally paper is cross shredded and/or incinerated. Jurisdictions may consider different shredding levels (area and width of shred particles) according to the confidentiality classification of the document.

Magnetic media

Magnetic media should always be treated and disposed of in a manner that is appropriate for the most sensitive data that has been stored on it during its lifetime. Media devices that will not be re-used (e.g. solid state drives, hard disk drives, USBs, disks) should be destroyed and reduced, usually by a grinding process with specialist equipment, to the point at which there is no usable material left.

If magnetic media will not be destroyed and will be re-used internally, appropriate actions should be taken to remove the existing information before re-use, or sanitise the media. Removable media not appropriately sanitised could put sensitive data at risk of being accessed by unauthorised users. Box 35 illustrates the importance of sanitising storage media. Tax administrations may decide on different methods, such as overwriting techniques, and can refer to international standards on media sanitisation for further guidance.

As it can be difficult to remove all evidence of data from a disk, it is not usually good practice, however to re use a disk that has held highly confidential information. In any event, tax administrations are recommended to hold records, normally part of the asset inventory (discussed in SR 3.2.4.3 on asset management controls), indicating the usage history of each device.

Box 36 provides examples of destruction procedures.

SR 3.2.5.2. Protection of exchanged information

This section is about measures to give effect in practice to the confidentiality and appropriate use provisions contained in international exchange agreements

Box 36. **Example of secure destruction of confidential information no longer needed**

Jurisdiction C's tax administration conducts mass destruction of paper and digital documents at least once per year, or when sufficient material has accumulated. It engages a contractor with specialist equipment for shredding (micro or cross shredding) and/or grinding. This process is set out in a written procedure for the destruction and disposal of official tax administration information:

- The material (paper or magnetic media) is entered in a log of materials for destruction. This log enables tracking the material through to the point where destruction has occurred and the fact of destruction has been verified and validated by designated tax administration personnel, appointed by a senior manager.
- Materials are securely transported to appropriate facilities and held securely for some time before the destruction event. The log of materials for destruction records the current location of material awaiting destruction and the person who is responsible for the material at that point in time. The responsible person is accountable for ensuring that materials are securely held, and carrying out appropriate checks that this is the case.
- Where material is earmarked for physical destruction and some time elapses before the destruction event, storage media are securely sanitised before they are stored, in preparation for destruction.
- Ahead of the day of destruction, a schedule is prepared detailing all of the material to be destroyed. A copy is sent to an independent witness, who approves that destruction can proceed. The witness is present throughout the destruction process, first to check the schedule as each item is removed from its secure storage, then to verify that each item is destroyed as prescribed in the procedures, then finally to confirm that all of the scheduled items have been destroyed as planned.

and domestic laws regarding exchanged information (see CR 3.1). To protect exchanged information, tax administrations may:

- Utilise the policies and practices developed to ensure confidentiality for domestic tax purposes also for exchanged information, e.g. applying the types of controls described in SR. 3.2.5.1.
- Develop bespoke and enhanced policies and practices specifically for exchanged information. These policies are sometimes incorporated into the EOI manual, and generally include:
    - Confidentiality classification and labelling of exchanged information.
    - Controls to access digital and physical EOI records.
    - Secure transmission of information to foreign competent authorities.
    - Secure transmission of information from financial institutions, in the case of the AEOI Standard.
    - Secure transmission of information from the competent authority or EOI unit to other areas within the tax administration or external parties.

Classification and labelling of exchanged information

Exchanged information, both sent and received, should be suitably classified as confidential and visibly labelled as such. Labelling is commonly achieved through a "treaty stamp" for paper EOI mail and files, or a watermark in case of electronically exchanged files (i.e. the marking indicates that the information has been exchanged pursuant to an international exchange agreement and is subject to its particular restrictions on disclosure and use, as described in CR 3.1).

A treaty stamp or watermark may state, for example:

"THIS INFORMATION IS FURNISHED UNDER THE PROVISIONS OF A TAX TREATY AND ITS USE AND DISCLOSURE ARE GOVERNED BY THE PROVISIONS OF SUCH TAX TREATY."

Controls for access to digital and physical EOI records received from foreign competent authorities

These controls may include:

- Only specific authorised personnel access EOI unit premises, bearing proper identification (e.g. electronic pass, photo-ID). Other employees only access the EOI unit with authorisation from the head of the EOI unit. Members of the public do not access it under any circumstances.
- EOI officers are subjected to enhanced background checks before commencing EOI functions and/or a higher level of security clearance (see SR 3.2.2 about human resources controls). IT staff involved with databases holding exchanged information are also subjected to enhanced human resources controls.
- Strict CDPs apply to all exchanged information in hard copy and mobile devices that hold it, and these must be stored in locked drawers or cabinets.
- Hard copies of exchanged information can only be printed by authorised individuals in the EOI unit, and should be labelled with a confidentiality and treaty stamp.
- Hard copies of exchanged information must be securely shredded when no longer needed.
- Enhanced domain controls are implemented around databases that hold exchanged information.
- Access to EOI systems and databases is restricted to personnel expressly authorised on a need to-know basis (see SR 3.2.3 on access management).
- All incoming requests for information and all information received are entered into an internal IT management system which can be accessed only by the authorised personnel via individual login and password. Accesses are logged and monitored (see SR 3.2.6.2 on log management).

Secure transmission of information to foreign competent authorities

Transmission is at the core of EOI. There should be specific controls when information is sent to or received from a foreign competent authority, whether on request, automatically or spontaneously.[17] The controls should extend to all related documents, communications and background information in relation to the exchange. The following controls may be considered:

- In case of EOI on request, confirming that a foreign official who has requested information is the competent authority or its authorised representative under the applicable international exchange instrument, therefore authorised to make the request and to receive the information, and confirming that their name and address/email are correct before sending any information.
- Secure transmission between competent authorities, for example:
  - Electronic transmission, whether on request or automatic, should be always secured with an appropriate level of encryption.
  - Only persons authorised to handle exchanged information should have access to the EOI mailbox, with password protection.
  - Physical mail should only be sent using an international registration system with mail tracking.
  - Mail received from a foreign competent authority should be delivered directly to the EOI unit.
  - Cover letters to the foreign competent authorities should emphasise the confidentiality of the information by including a statement on the applicable treaty restrictions on disclosure and use (see example above).

Secure transmission of AEOI information from financial institutions

The electronic transmission of information from financial institutions to tax administrations with respect to the AEOI Standard should be suitably encrypted.

In addition, there should be mechanisms to certify and authenticate the financial institutions. This is usually achieved through multi-factor authentication and/or digital signature.

Secure transmission of information from the competent authority or EOI unit to other areas within the tax administration and external parties

It is often necessary for exchanged information to be sent by the competent authority or EOI unit to other tax officials or authorities within the tax administration, or external parties (e.g. public prosecutor). A record should be kept showing who the information has been disclosed to, how many copies have been produced and who has a copy in their possession at any time.

In many cases, the competent authority or EOI unit receives large amounts of information regarding many taxpayers, and often only a portion of that information is required by a specific tax compliance auditor or similar official in a certain region of the country. Competent authority or EOI unit personnel are responsible for ensuring that only the specific information needed by the particular individuals is forwarded and that bulk information is not simply retransmitted.

As discussed above, treaty stamps and warnings are often used to protect confidentiality of the information when sent by one competent authority to another. Competent authorities who then forward that information within the tax administration may also include warnings. In addition to stating that the information is confidential and has been obtained under a tax treaty, warnings may advise that the information may not be disclosed under freedom of information laws or without consulting the relevant foreign competent authority in advance. This is to help ensure that unauthorised disclosure does not occur.

Some jurisdictions include warnings on the cover page and others include the warning on each page of the information in case pages become separated. Where the exchange agreement allows the information to be used for other (non-tax) purposes, the receiving law enforcement agencies and judicial authorities must treat that information as confidential, consistent with the agreement (see CR 3.1).

[17] For more detailed information on policies and practices to protect the confidentiality of exchanged information, see "Keeping it Safe: The OECD Guide on the Protection of Confidentiality of Information Exchanged for Tax Purposes", www.oecd.org/ctp/exchange-of-tax-information/keeping-it-safe-report.pdf

Box 37. Example of controls to protect exchanged information

In Jurisdiction A's tax administration, all staff who deal with exchanged information are security cleared and trained on EOI. EOI data are classified as "Confidential". Security controls are commensurate with this classification, and all information in physical or digital format is clearly labelled as "treaty protected".

Incoming and outgoing EOI requests are handled by the EOIR Team, and information exchanges under the AEOI Standard are handled by the AEOI Team. The EOI manual guides tax officers in the handling of incoming and outgoing EOI requests as well as AEOI information.

EOIR information received is segregated from other taxpayer information, and can only be accessed on need-to-know basis. Information received via the AEOI system is stored separately from other taxpayer databases and is accessible by authorised administrators on a need-to-know basis, with multi-factor authentication.

In addition to the physical access measures in place, physical documents, records and storage media (such as CDs and USB sticks) received from exchange partners are securely kept in unmovable multi-lock cabinets within the EOIE/AEOI Team premises.

Information sent to exchange partners electronically is always encrypted.

For incoming EOI requests received from exchange partners, only the minimum information in the EOI request letter is disclosed and forwarded to local tax offices, for the purpose of enabling the local tax auditors to obtain the requested information from the information holder. Local tax auditors must confirm in writing that the data will be kept confidential and will only be used in accordance with the applicable international exchange agreement. Local tax auditors are also trained on the use of the EOI manual and on the handling procedures for exchanged information.

The following warning is included when information is forwarded to local tax offices: "All information received under the exchange of information provisions of a treaty may only be used for tax purposes, unless specifically authorised for use for other purposes, and must be maintained in the strictest confidence. Disclosing these documents, including under the Privacy Act or Freedom of Information Act, must be discussed with the EOIR team prior to disclosure. Section 1 of the EOI manual provides further guidance."

Exchanged information is archived for 10 years when no longer needed for work purposes, beyond which it is destroyed. A designated employee from the tax administration witnesses the entire destruction process.

Box 37 illustrates with examples the (enhanced) controls that can be applied to exchanged information.

SUB-REQUIREMENT 3.2.6: OPERATIONS MANAGEMENT FRAMEWORK, INCLUDING INCIDENT MANAGEMENT, CHANGE MANAGEMENT, MONITORING AND AUDIT

SR 3.2.6 focuses on the "check" component of the PDCA lifecycle. In other words, the operational arrangements used by tax administrations to verify that the ISM system and its controls are working.

While, in general, security operations can be very broad, the AEOI confidentiality assessments highlight and focus on some of the critical capabilities, processes and controls that tax administrations are expected to have in place, particularly in the IT area. These operational controls cover the following areas, starting with a general outline of the operations management framework tax administrations are expected to have in place, followed by guidance for the controls in six areas of operations management:

- SR 3.2.6.1: General operational management framework.
- SR 3.2.6.2: Log management.
- SR 3.2.6.3: IT risk management.
- SR 3.2.6.4: Vulnerability management.
- SR 3.2.6.5: Change management.
- SR 3.2.6.6: Incident management.
- SR 3.2.6.7: Internal and external audit.

Table 24 provides definitions of the main concepts covered in SR 3.2.6.

SR 3.2.6.1. General outline of security operations management framework

Effective coordination of operational security activities is an important enabler of the key strategic processes regarding security, such as the ISM system and corporate risk management. It is key for a tax administration to have visibility of what the messages the operational processes are conveying from their day-to-day functioning,

Table 24. **Glossary of main concepts**

Concept	Description
Audit function	Comprehensive, unbiased reviews to assess compliance with ISM system processes established in policies and procedures. Audit findings and results should be directly reported to the head of the tax administration.
Change management	Refers to the controlled management of the development of new systems and services, and making major changes to existing ones.
Incident management	Entails identifying, documenting and managing security incidents, both in the IT and non-IT areas.
Log	A log, in a computing context, is the automatically produced and time-stamped documentation of events relevant to a particular IT system. Manual logs can be created for non-IT activities as well.
Log management	Refers to the collective processes and policies used to administer and facilitate the generation, transmission, analysis, storage, archiving and ultimate disposal of the large volumes of log data created within an IT system.
Logging	Logging refers to tax administrations recording and keeping track of all access to protected data, including access to facilities and areas where the data is held, and in particular to systems that hold taxpayers' records and other sensitive information.
Security Operations Centre	A Security Operations Centre is a team of specialised professionals and systems for monitoring and analysing the security posture of the tax administration on an ongoing basis.
Vulnerability management	Refers to the processes and procedures for the identification and management of vulnerabilities.

including in relation to security controls (including those that protect exchanged information). SR 3.2.6.1 therefore requires tax administrations to be aware of the controls that protect exchanged information, and have appropriate plans in place to manage them.

A "Security operations management framework" can be defined as a collection of interconnected operational practices that help to maintain the ongoing security posture of the tax administration. It consists of the operational arrangements for the monitoring, maintenance and management of the security aspects of the IT estate, its people, and its processes.

The scale of a security operations management approach will depend on the size of a tax administration and the complexity of its operations, for example:

- Larger tax administrations, with complex and diverse operations, may have the individual functions of operations management (logging, security risks, vulnerability management, change management, incident management and audit) split across IT systems, business services or support teams, with a centralised unit for the management of threats to operations.
- Smaller tax administrations may have insufficient complexity to justify centralised planning, and there may be operational managers responsible for each of the individual functions of operations management.

Whichever the scale of the tax administration, the important point is that operation management activities should be effectively planned and coordinated across areas.

Therefore, there should be in place an overall security operations management approach, clearly reflected and documented in the set of domain-specific policies (as described in SR 3.2.1) in which the broader context of the ISM framework is outlined.

The domain-specific policies should include reporting arrangements under which operational managers provide periodical reports to the ISO, or raise alerts about the performance of the domain-specific security controls in order to ensure that regular activities are carried out as necessary to effectively mitigate risks (and risks should be reflected in a risk register on an ongoing basis, as described in SR 3.2.1.4).

In practice, the approach to operations management is often centralised in a Security Operations Centre (SOC). A SOC comprises a team of specialised professionals and adequate systems for monitoring and analysing the organisation's security posture on an ongoing basis. A SOC team's goal is to detect, analyse, and respond to security incidents using a combination of technology solutions and incident response activities.

The following sections explain the key functions of operations management in each of the six relevant areas.

SR 3.2.6.2. Log management

Logging refers to tax administrations recording and keeping track of all access to protected data, including access to facilities and areas where the data is held, and in particular to systems that hold taxpayers' records and other sensitive information. Log management refers to the collective processes and policies used to administer and facilitate the generation, transmission, analysis, storage, archiving and ultimate disposal of the large volumes of log data created within an IT system.

Tax administrations should ensure that access is fully logged, monitored and retained for a sufficient time to fulfil control requirements such as transaction monitoring, incident management and audit.[18]

Logging serves at least two purposes: to monitor the effectiveness of the controls, and to provide evidence in case an incident occurs.

SR 3.2.6.2 therefore requires that tax administrations have appropriate logging and monitoring arrangements in place, including to detect unauthorised access, use or disclosure of information.

Tax administrations should, in particular, determine their logging and monitoring approach for exchanged information, which could either follow the general logging framework, or be part of a dedicated logging and monitoring approach.

Tax administrations should:

- **Record logs**. Recording logs is a very important proactive tool enabling logs to be referred to in case of malicious activity or unlawful access, and allowing malpractice to be traced back to the person(s) responsible. If properly recorded and retained, logs can be used as evidence for sanctioning procedures, whether administrative or criminal.
- **Monitor logs**. Log monitoring helps identify and take appropriate action in relation to suspicious activity before a major incident happens. For example, there may be activities that monitoring would identify which, while not constituting an incident, might nonetheless be a cause for concern, such as frequent requests for password restoration. This activity, by itself, involves no breach of policy, but it might be a signal that employees have low awareness of good practices for password management and are generating passwords that they cannot remember, or that the guidance from the IT department on how passwords should be structured to meet the complexity criteria are not clear.
- **Protect and store logs**. Logs themselves are an important information asset that needs to be protected and stored, in line with legal and security requirements. Legal requirements may include retention periods for the logs, which should be defined and documented. If not defined by law, the recommended retention period should coincide with the review period for logs, and not less than 3 months. Tax administrations should have the capacity to retrieve logs and interpret them as needed, and this should be tested on regular basis. The security requirements can cover implementation of access controls for the logs, review of access rights, inclusion of logs in backups, hashing for integrity control, log destruction, etc.[19]

Tax administrations should also clearly identify which activities should be logged and establish procedures for log monitoring and for management of evidences.

What activities should be logged?

Based on an assessment of information security risks (see SR 3.2.1.4 on risk management), an ISO, in coordination with the head of the IT department,

[18] Logging and monitoring is also covered as a baseline IT control in SR 3.2.4.2, referring to IT security controls.

[19] Destruction of logs should follow a predefined procedure for secure destruction or disposal, as explained in SR 3.2.5 on the protection of information.

should identify:

- What activities should be logged.
- How often logs should be reviewed.
- The parameters for their monitoring, so that alerts are sent in case of a suspected incident.

Log recording and monitoring can cover IT and non-IT activities, such as:

- **Internet traffic.** Monitoring the origin of IP addresses, in particular IP addresses that are linked and of foreign origin, is important information in particular in the tax administration context, where the vast majority of connections are expected to be domestic and/or conforming to certain types.
- **Malware prevention software.** Monitoring of logs from antivirus software can identify if some virus is repeatedly infecting a system and can indicate the need to block the origin of where it comes from. Conversely, if logs indicate that few viruses are being blocked, this might mean that the software is not updated with the latest list of virus definitions.
- **Firewall.** Monitoring data traffic from the tax administration outwards might identify unexpected flows that should be checked, e.g. determining whether an outflow to a private company or a newspaper is legitimate.
- **Access management.** Monitoring of domain logs for access should look for authorised and unauthorised accesses. Special focus can be placed on access from unregistered or unexpected devices (e.g. authorised users from a private device), or multiple attempts of unauthorised access (e.g. indicating a penetration attack or a denial-of-service attack).
- **Databases.** Monitoring database logs can detect unexpected or unauthorised changes to data, access to sensitive databases by authorised users and/or access attempts by unauthorised users.
- **Physical access.** Monitoring CCTV and other electronic access controls, as well as accesses to confidential paper documents or restricted premises (e.g. an EOI unit), can detect intrusions. These types of logs can be kept manually, with less automated processes, but should nevertheless follow the same reviewing, monitoring and storage procedures as automated logs.
- **Compliance with security controls in the office environment.** Logging fire extinguisher certification, keys distribution etc.

Log monitoring and management of evidences

Tax administrations should monitor log records regularly. Monitoring can be passive, i.e. monitoring after an event or incident occurs, or active, i.e. systematic monitoring or monitoring of logs in real time, using log management systems.

Active monitoring, in particular, may be done to different degrees, such as:

- **Alerts.** Parameters can be set so that if certain events occur, they can be identified as they happen, investigated, and if necessary immediately terminated. Such events might include an unexpected rise in internet traffic, an unexpected type of traffic, or significant volumes of data being ex-filtrated. Tools such as data leakage protection can be used for alerts.
- **General monitoring.** A good example is real time monitoring of CCTV for breaches of security. General monitoring could equally include simply monitoring internet traffic for unforeseen events, for which no alert has been set up.
- **Work lists.** Triggers are set for events that require reviewing, and when these happen a notification will be added to a work list and the event will be reviewed in normal office hours, where possible within one working day of the event occurring. This form of monitoring is intended for events that require action or control, but which are not critical, for example because they only affect a single record. This type of active monitoring might best be described as 'near real time' and is relatively closer to the passive monitoring category.

An organisation would generally make a selection of passive and/or active monitoring methods as informed by factors including:

- Assessed risks.

- Security and business requirements.
- Monitoring personnel's skills.
- Log storage capacity.
- Quantity of logs, and the dynamics of their generation, as this might have budget implications.

Tax administrations should also consider the following practices in log monitoring and management of evidences:

- **Defining reporting parameters between what is considered an event that requires urgent or priority reporting, and non-urgent events which do not need to be prioritised.** For example, alerts could be established only for sensitive log sets (e.g. logs of access to CRS databases) for which failures would have more serious consequences. Alerts triggered by the access control system could be linked to the incident management procedure covered under SR 3.2.6.6.
- **Having controls in place to protect the integrity of logs when utilised and analysed.** This includes hashing to ensure the integrity of the logs, backing up logs on regular basis and imposing strict access control in relation to the persons who can see or manage logs.
- **Reviewing monitoring controls.** Reviews should be done on a regular basis so that adjustments can be made in alerting criteria.
- **Clearly defining the roles and functions of relevant persons with respect to logs.** This includes the persons responsible for the activities of log monitoring, reviewing log file access and access rights, and determining the controls to protect log file integrity. These persons may include the ISO, IT officers, the SOC or an external provider where applicable. The organisation should document under what circumstances persons are authorised to utilise and analyse log records, e.g. the ISO for the analysis of incidents or for measurement of the effectiveness of implemented security controls, or the compliance or internal audit department for the investigation of a reported incident of misuse of information.
- **Having defined policies or practices for retaining logs and for the management of evidences.** This enables the "chain of custody" of data or documents impacted to be maintained, so that proper investigations can be carried out under internal disciplinary procedures or by law enforcement authorities. Such policies or practices will include log management policies with controls for retention, integrity, and access, as well as detailed procedures for maintaining and protecting evidence by using copies, encryption and backup.

Logging and monitoring can be scaled and managed using tools such as SIEM systems, if an adequate cost benefit can be achieved for the tax administration. See Box 38 for an example of a logging and monitoring approach in a tax administration.

Box 38. **Example of logging and monitoring**

All systems of Jurisdiction A's tax administration log all accesses to data (failed or successful attempts). A centralised logging system logs and records all activities. Access to the logs is also logged. There are special protections to maintain the integrity of logs and prevent unauthorised changes to log files. Logs are retained for 18 months.

The monitoring of logs and its frequency are based on the organisation's data classification system. Logs of systems that contain data classified as sensitive or confidential and which are accessed by users with administrator's rights, e.g. AEOI systems, are monitored through a specialised system for real time monitoring, which provides alerts when suspicious activity is detected. There is also a more passive approach in place to review logs of non-sensitive systems and non-privileged accounts, and they are reviewed according to pre-defined schedules or when required.

The ISO regularly reviews logs from the various systems to check the effectiveness of the controls established for the system. The ISO, working with the incident management officer, also reviews logs as part of incident response and analysis, aiming to understand not only the impact and cause of the incident at hand, but also the underlying problem that raises risks.

SR 3.2.6.3. Operational management of IT security risks

The operational management of IT security risks is a key activity in a tax administration's environment, as IT threats can have large-scale and profound impacts if they compromise databases holding sensitive information.

A tax administration's approach to IT security risk management should be compatible with the general risk management process used as described in SR 3.2.1.4, i.e. the overall risk management methodology, both for IT and non-IT activities.

Tax administrations should consider the following specific aspects (see Box 39 for an example of management of IT security risks):

- **The IT department's involvement in the overall risk management process.** It is critical that the IT department is fully involved in the tax administration risk management processes, since most, if not all significant business risks will have an IT dimension. This is particularly important for the identification of the most suitable controls, as well as an evaluation of the impact or effectiveness of those controls in actually lowering the identified risks. Ideally, the IT risk register should be integrated with the business risk register. Such integration can provide for increasing the visibility of IT risks in the overall risk arena, as well as understanding of the impact of changes in the business risk on IT and security controls.

- **The IT consequences of business management decisions.** Due to the increasing reliance on IT in every aspect of tax administrations' operations, most business decisions have IT implications, i.e. require some change or modification of an existing IT system. These implications should be well analysed and considered in relation to the security of data. Business decisions regarding the funding of the IT department can also have significant impact on security, as security is based on the controls that are operationally managed by IT.

- **The risk consequences of IT decisions.** During the design, development and implementation of new IT applications and infrastructure, or during regular IT system enhancements, IT personnel should continually think about the changes in the overall risk environment that such developments or changes might lead to, and adequately reflect their conclusions in the risk register.

- **Regularly monitoring IT risks and reviewing IT security controls.** As the IT environment is constantly changing, new risks, threats and vulnerabilities are continuously arising and being identified by IT professionals. IT personnel should therefore monitor developments on a daily basis and regularly review their IT risks and the validity of the controls in place (see also SR 3.2.6.4 on Vulnerability Management).

- **The approach regarding external providers of IT services.** Where IT is managed outside the tax administration, adequate agreements and SLAs should govern the relationship with external providers and their provision of IT services, covering how risks in the provision of those services are managed and reported. Those risks should be integrated into the tax administration's own risk management.

Box 39. Example of management of IT security risks

IT security risk management in Jurisdiction B's tax administration is carried out by a risk assessment team comprising the ISO and representatives from the IT department and business areas. Team members, under the leadership of the ISO, jointly identify IT security risks and assess their likelihood of occurrence and potential impact. Risk acceptance criteria are predefined by senior management on the ISO's advice, and reflected in the team's risk assessment. All risks outside risk acceptance must be addressed with controls.

The IT department provides the technical input and proposes controls to mitigate risks identified, while the ISO ensures that the controls are consistent with information security policies and procedures. Business area representatives provide input to ensure that the controls will not affect the overall performance of their business processes.

The risk assessment and selected controls are recorded in a risk register. The team regularly reviews the assessment, and an IT manager is required to keep track of the implementation of the IT mitigation controls and their effectiveness.

SR 3.2.6.4. Vulnerability management

SR 3.2.6.4 requires tax administrations to have processes and procedures for the identification and management of vulnerabilities. Vulnerability management refers to periodically scanning the organisation's IT environment to identify vulnerabilities that would pose a significant security risk. Appropriate IT security controls should be deployed to manage vulnerabilities identified (see discussion in SR 3.2.4.2).

The frequency and scope of vulnerability scanning will depend on a tax administration's complexity and scale of IT operations, its identified risks, and available budget. Regardless of the frequency and scope, the vulnerability analysis should be thorough in order to determine the policies or controls in the ISM system that need improvement. Although there are various tools available to identify vulnerabilities, SR 3.2.6.4 focuses on vulnerability scanning and penetration testing of IT environments.

Vulnerability scanning

Vulnerability scanning refers to the identification of design flaws in IT systems that are prone to abuse by some internal or external threat agent. A scanning tool automatically checks for possible entry points through which hackers may enter into programs, services, or ports, and for faults in the construction of an IT infrastructure.

There are various types of vulnerability scanning tools, depending on the desired scope and depths of scanning. They can include:

- **Network vulnerability scanning:** the check-up of all systems in the network and computers to detect security loopholes.
- **Unauthenticated and authenticated scans:** scanning of systems for vulnerabilities can be done simulating an external hacker without user credentials (unauthenticated scan) or with user credentials (authenticated scan), the latter being the case of a hacker who already has user access to the system.

A vulnerability scanning report should be immediately analysed, and the identified vulnerabilities addressed by adequate controls.

Penetration testing

Penetration testing, also called "ethical hacking", is a particular type of vulnerability test that checks the possible scope and depth of access by an unauthorised user at a given point in time. All tax administrations, regardless of their scale, are expected to regularly penetration test both external and internal interfaces. Interfaces handling AEOI data should be regularly penetration tested.

To effectively penetration test, tax administrations should consider the following aspects:

- **Penetration testing both internal and external interfaces.**
  - **External interfaces.** The penetration test focuses on the connections between the world and the IT system of the tax administration.
  - **Internal interfaces.** The penetration test focuses on the internal connections within the tax administration's platform or IT system to make sure the "need to know" and "least privileged access" principles are adequately implemented.
- **Periodical penetration testing.** A penetration test tests systems at the given point in time when the test is performed. Penetrations tests are therefore of most value when testing new systems or major system changes, both before and immediately after they go live. Critical interfaces should be penetration tested at regular intervals, at least annually or even more frequently depending on their importance.
- **Engaging independent and reputable third-party penetration testers.** Ideally, penetration tests should be carried out by a third-party penetration test provider independent from the tax administration. It is important to employ reputed penetration testers with proved experience and knowledge of the latest techniques. It is advisable that certified ethical hackers are engaged.
- **Establishing clear requirements with the penetration tester.** The success of penetration tests is very dependent on the quality of engagement with the tester. Tax administrations should always enter into a contract with the penetration tester before the tests are carried out, and establish a non disclosure

agreement in relation to information the tester might eventually see, with their agreement not to misuse it. The contract should include pre-determined constraints within which the tester will work, such as the kind of equipment they should use and what information about the tested system the tester will be provided with. Depending on the parameters defined, tests can be "black box" (no information on the system except the website address is given) or "white box" (the tester is made aware of the infrastructure and system setup). Test requirements should be discussed with the penetration tester openly, giving them the opportunity to consider the business context in which the tax administration operates and to offer suggestions. Because of their experience, penetration testers may have a better idea of the current threat horizon and will be able to suggest alternatives in relation to the approach and scope of a test.

See Box 40 for an example of vulnerability management controls.

Box 40. **Example of vulnerability management controls**

Jurisdiction C's tax administration scans all systems, applications and databases to detect potential vulnerabilities that could be exploited by a potential attacker, and applies controls accordingly. All traffic between the web, applications and databases is monitored 24/7 by physical firewalls and specialised systems that provide real-time updates on potential attacks, so that these can be detected and responded to in a timely manner.

The tax administration also engages specialised security firms to conduct ethical hacking on both internal and external interfaces. AEOI systems are penetration tested annually. All new applications have to go through web penetration testing before they go live, and all findings and vulnerabilities must be fixed before launch.

SR 3.2.6.5. Change management

Change management is the controlled management of the development of new systems and services, and making major changes to existing ones. It covers sound solution design, testing and release control, and is the means by which it is ensured that IT security is built into systems changes.

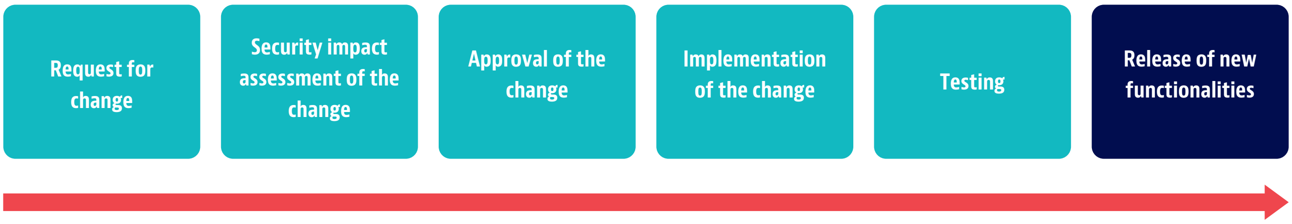
SR 3.2.6.5 requires that tax administrations have a change management process, with security integrated into it. The process can be documented in a policy or a procedure depending on the level of detail needed, and should be reviewed by the ISO at regular intervals.

Viewed from a security perspective, the change management process itself is a high-risk activity. Changes to systems without an adequate IT security approach could result in vulnerable systems and lead to major security breaches. This could include changes rushed through because of budget and time restrictions and without project discipline, inadequate testing and with warnings ignored.

A sound change management approach should therefore be developed and implemented jointly by the IT department, business systems owners and users, and the ISO. It should include the sequence of key steps depicted in Figure 18:

- **Request for change.** All requests for changes should be documented with an indication of the expected benefit from the change, the systems or processes involved, problem(s) that it solves (if it is based on some incident or known vulnerability), the urgency and deadlines, and the level of priority and criticality for business processes.

FIGURE 18. **Steps of change management**


Request for change
Security impact assessment of the change
Approval of the change
Implementation of the change
Testing
Release of new functionalities

Tax administrations should clearly define the types of changes that can be requested, and the criteria for each. The two main types include:

  - **Regular changes.** These are changes that can be planned, prioritised, approved, tested and released. They can be further separated into minor and major if appropriate.

  - **Emergency changes.** These are changes that have to be implemented immediately to solve some critical deficiency, where delays in implementation may cause more damage. The ordinary steps in the change process are skipped and taken after the implementation of the change. Often, emergency changes happen as a result of an incident. The incident management process is described in the following section, SR 3.2.6.6.

- **Security impact assessment.** The various implications of the change on the business process, IT and security should be assessed by the personnel involved in each of those aspects. There should be a balance between the functionality that the business needs, the controls for risk mitigation that the ISO recommends, and the technological advances or limitations posed by the system.

- **Approval of the change.** Usually allocated to the ISO or senior management, the responsibility for approval of changes can be defined as part of the roles and responsibilities in the ISM policy (see SR 3.2.1.2).

- **Implementation of the change.** During implementation, the teams involved should ensure that the security requirements are met prior to release. For example, if changes are made in source code of software, the integrity of the source code will be managed using code versioning tools. If the change involves processes or procedures, there should be alignment with the overall ISM policy and other relevant policies.

- **Testing.** Testing changes is critical, especially if they are implemented on IT systems. Where possible, testing should not be done directly in the production environment. In case of changes to software, testing should be done in an isolated environment with dummy data. This allows for errors and mistakes without risk to real data and/or to the actual functioning of processes. Clear guidance on the use of data for testing should be established in policy, as well as on the criteria to release changes.

- **Release of new functionalities (change release).** The release of a change should be a planned activity whenever possible. This means that the release of new functionalities should be done during periods when disruptions to the tax administration's business operations will be minimal. It is good practice to release changes with a ready rollback plan, i.e. a plan on how to go back to or restore the previous mode of operations in case the release to production of the changes is unsuccessful.

Poorly executed change is a major cause of incidents, including security incidents. Adequate governance should therefore be in place. This will be partly achieved by having an entity formally authorising change release, e.g. the ISO or, in more complex organisations, a Change Control Board or equivalent body including representatives of different operational areas, including security. Such an entity will ordinarily develop a forward change schedule, circulated to all relevant stakeholders periodically, to provide visibility of upcoming changes and help avoiding disruption to business activities.

An ISO should regularly review the organisation's approach for change management, to verify its effectiveness. See Box 41 for an example approach to change management.

Box 41. **Example of change management**

Jurisdiction A's tax administration has detailed guidelines for change management and code review. The guidelines take into account the requirements of business users and the IT department, including information security.

All changes, including source code, are first tested by developers in a development environment. IT senior managers then carry out new tests in a test environment, to which developers do not have access. The release can be deployed into production only after these two tests have been performed.

All source codes are securely stored in a secure repository with privileged access given to persons on a strict need-to-know basis.

SR 3.2.6.6. Incident management

SR 3.2.6.6 requires tax administrations to have an incident management system that covers all types of security incidents. Incident management entails identifying, documenting and managing security incidents, both in the IT and non-IT areas.

An incident essentially means something happening that is not supposed to happen. Even if tax administrations implement controls well, things may not go as planned. There are two main reasons to have an Incident Management system:

- To remedy incidents as speedily and effectively as possible, to minimise their possible impact.
- To prevent incidents from happening again.

Incidents across different areas of a tax administration should be managed in a similar way even if they are not all managed by the same people. For example, IT incidents are normally managed through an IT help desk. Non-IT security incidents, such as physical access incidents or security pass incidents, might be handled by the unit responsible for building and facilities management. Other incidents might be handled by the human resources department, or through internal audit.

There should exist, in any case, a documented policy or procedure defining the approach for the management of all security incidents affecting the tax administration. This is primarily so that the security team and others involved can consider possible links between different types of incidents, to look for patterns that might point to risks that have not yet been considered.

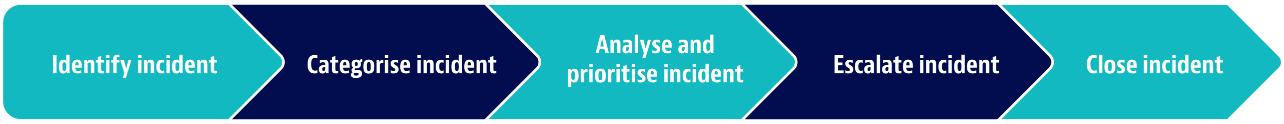
The tax administration's incident management approach should be clearly communicated to all personnel. In addition, a clear responsibility for managing incidents should be documented as part of the roles and responsibilities in the ISM policy (as described in SR 3.2.1.2) related to the overall security framework.

The approach to incident management should generally follow a series of steps, which can be translated in the form of a workflow depicted in Figure 19.[20]

- **Identify IT and non-IT incidents.** Personnel should be encouraged to report any events, both IT and non-IT, that they think can be security incidents. Channels to report incidents should be accessible by all personnel, and procedures should not be burdensome. Incident reporting should be covered in induction or security awareness training for all personnel. Incidents are also identified as part of log monitoring activities (see SR 3.2.6.2).
- **Categorise incidents.** The person(s) responsible for managing incidents should review reported incidents and categorise them so that adequate action can be taken. The categories, which should be documented in policy, can include:
  - Information security incidents, or events that can result in negative outcomes from an information security point of view, i.e. they affect the confidentiality or integrity of information. For example, an USB device containing confidential information is lost or stolen, or electronic ID of personnel in the EOI unit is lost.
  - Other incidents, for example an IT incident without information security impact, such as a malfunctioning printer.

  Based on the category of an incident, its resolution might be coordinated by ISO or the IT Help Desk or both, as documented in the incident management procedure.
- **Analyse and prioritise incidents.** Based on their potential impact, security incidents should be analysed and classified as minor or major incidents, so they can be prioritised for remediation. The criteria

FIGURE 19. **Incident management workflow**



[20] More detailed guidance can be found in international standards such as ISO20000 or ISO27035.

for prioritisation can include the type of incident (e.g. electronic ID lost, USB lost or stolen), the type of information affected (e.g. internal memo, taxpayer, or exchanged information), the number of sensitive records involved (e.g. single datum, whole data set) and the likelihood of harm if information is disclosed (e.g. financial fraud).

Depending on its priority, the response time to a security incident might vary, and major incidents could trigger an escalation procedure.

- **Escalate security incidents.** If incident analysis shows that a major security incident has occurred, the incident should be escalated and investigated following established procedures, so that key stakeholders can be alerted (e.g. affected data subjects, data providers, authorities, foreign tax administrations in case the incident involves exchanged information, etc.). The escalation and communication to other authorities, depending on the scale and impact of an incident that is a confidentiality breach, should follow national legislation and other statutory or contractual requirements. More detailed guidance on these procedures is covered in CR 3.3, related to provisions and processes to address confidentiality breaches.

- **Close incident.** Closing an incident involves its remediation, the resumption of normal operations and a follow-up assessment of the incident. Depending on the scale of a security incident, the assessment should identify its primary causes, the processes that failed, the parties involved, the systems affected, the time to resolution, and the effectiveness of the solution implemented. This assessment is important to inform longer term strategies to further mitigate the likelihood of a security incident reoccurring in the future, or to reduce its damaging impact. Where warranted, non-compliance penalties and sanctions should be imposed, as described in SR 3.3.2.

The defined approach for incident management should include a regular review of its effectiveness. The ISO, together with the head of the IT department and representatives from business areas should review reported events, the incident classification and their closing. The analysis should result in the identification of issues or problems that are the source of recurring incidents, so that more systematic solutions can be implemented.

SR 3.2.6.7. Internal and external audit function

The internal audit function has an important role in information security in all organisations, including tax administrations, as it provides:

- **Process assurance.** Internal audit can detect process flaws that might increase the risk of data or information leakage and identify needs for improvement.

- **Process (non-)compliance.** Internal audit checks if personnel are complying with the ISM system processes established in policies and procedures, prompts improvements where the practice is different from what is established, and where necessary leads to disciplinary measures in case of non-compliance. Although managers and/or the human resources department usually handle issues involving employee misbehaviour and information unlawfully accessed, a properly functioning internal audit function will have the resources and expertise that will often enable it to identify the traces of non compliance before it becomes apparent to others. The internal audit approach should be documented and the competence of internal auditors should be ensured.

Tax administrations should establish policies and procedures for internal audit that observe the following critical principles:

- **Independence.** Auditors must not be beholden to any vested interest, other than the overall objectives of the tax administration as determined by legislation and the clearly stated policies that have been put in place to fulfil those objectives.

- **Access to evidence.** Auditors should obtain evidence on the effective implementation of the ISM system through interaction with personnel responsible for the activities. In case of suspicion, they can request direct access to the data, systems, and controls in question.

- **Access to key decision makers.** The head of internal audit should have direct access to the head of the tax administration if circumstances require.

- **Discretion on what to audit.** Although it is good practice for the head of internal audit to meet periodically with senior managers of the tax administration to identify suitable processes or functions for audit, internal audit should have control of at least part of its work programme and be able to audit those processes and functions that it considers most appropriate. The highest focus should be given to processes that pose the highest risk, but all processes should generally be reviewed, if not within the year then in some mid-term period.

- **Reporting of audits.** The audit report should present the findings on the general level of compliance with the different processes related to ISM, and propose recommendations for improvement. Corrective measures proposed should be coordinated with the ISO for implementation. The report should also indicate the sample of processes that was audited and the personnel involved in the audit, and be presented to senior managers of the tax administration.
- **Periodicity of audits.** Internal audits should be carried out on regular intervals. Depending on the complexity and size of the tax administration, the processes that pose the most risks to security should be assessed by internal audit at least annually.

In addition to the internal audit function, international good practice would require tax administrations to be subject to external audits carried out by other independent authorities in relation to the ISM system (e.g. Inspectorate General of the Ministry of Finance, State Audit Authority, Data Protection supervisory body, etc.).

In jurisdictions where the tax administration is small and it may be difficult to resource the internal audit function, reliance may need to be placed on the various external audit performed by the independent authorities in that country or on a commercial external audit performed by an accredited certification body.

Box 42 provides an example of internal audit of IMS processes.

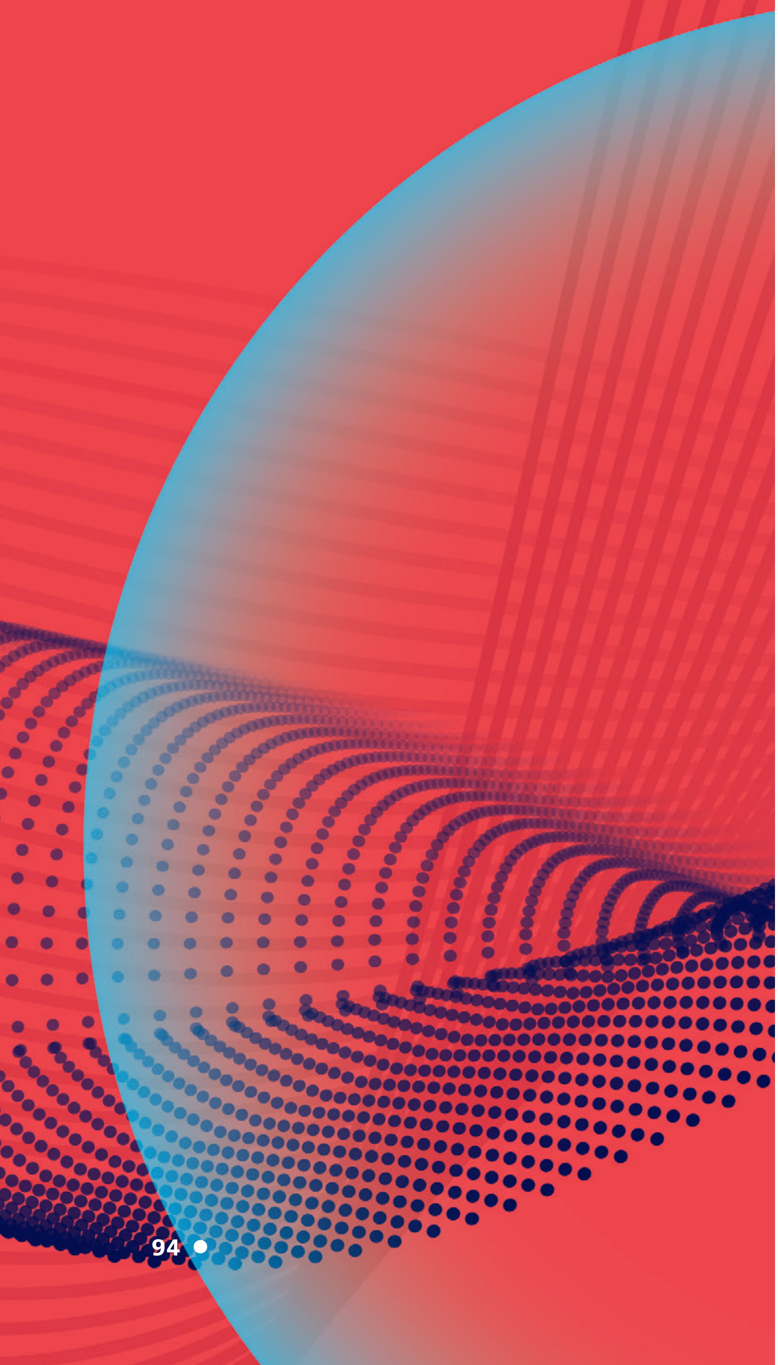
Box 42. Example of internal audit of ISM processes

The internal audit function in Jurisdiction B's tax administration has the objective of providing independent and objective assessments of the effectiveness of governance, risk management and internal controls within the tax administration. Audits are risk based and include, among others, audits of IT systems and processes, cybersecurity, data and information management, third party management and physical security.

Internal audit reports to the Comptroller General, and has unrestricted access and communication with the head of the tax administration. Audit results are reported to the Comptroller General on a quarterly basis and to the Commissioner on a half-year basis.

Audits on processes that involve EOI cover the review of logs and log monitoring and integrity, in particular access to taxpayers' information to ensure controls and procedures are in place and working as intended to prevent unauthorised access.

4. Enforcement provisions and processes to address confidentiality breaches (Core Requirement 3.3)



Even if appropriate ISM frameworks and security controls are in place, the possibility of unauthorised access or breaches of information cannot be ruled out. Effective enforcement provisions, and well-defined processes to manage and learn from confidentiality breaches, are therefore key to an ISM framework's robustness and a tax administration's ability to prevent future breaches.

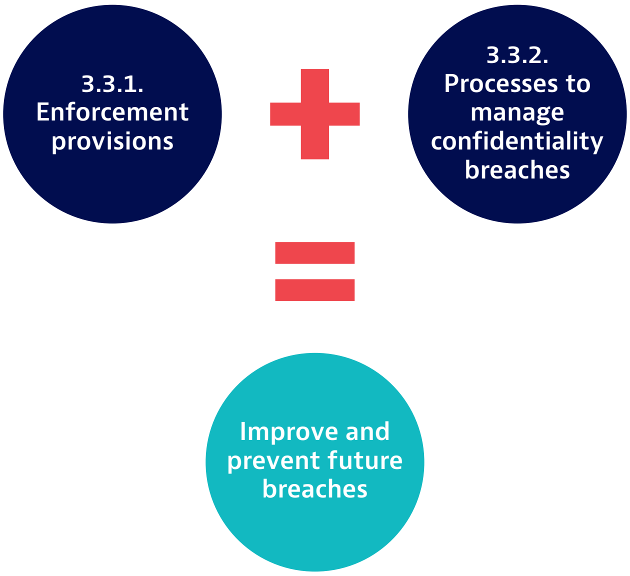
CR 3.3 therefore requires jurisdictions to have enforcement provisions and processes to address confidentiality breaches. It is divided into two SRs (see Figure 20):

- SR 3.3.1: Jurisdictions should impose appropriate penalties or sanctions for improper use or disclosure of information.
- SR 3.3.2: Jurisdictions should apply appropriate processes to deal with suspected or actual non compliance, including effectively applying sanctions

SUB-REQUIREMENT 3.3.1: SANCTIONS FOR IMPROPER DISCLOSURE OR USE OF TAXPAYER INFORMATION

To ensure that the legal provisions on the confidentiality and proper use of taxpayer information, including exchanged information, are given effect, the law should impose sanctions that are clear and severe enough to

FIGURE 20. **Core components of addressing confidentiality breaches**


3.3.1. Enforcement provisions
+
3.3.2. Processes to manage confidentiality breaches
=
Improve and prevent future breaches

Box 43. **Example of sanctions for unauthorised disclosure or use of taxpayer information**

Jurisdiction A's Income Tax Act (ITA) establishes monetary and criminal sanctions, depending on the seriousness of the offense, for any person, including personnel and external contractors, who violates the confidentiality of taxpayer information under the ITA. Violations are punishable by a fine of up to EUR 15 000 or imprisonment up to three years.

Under the Jurisdiction A tax administration's Code of Conduct, the unauthorised disclosure or use of taxpayer information, including exchanged information, constitutes major misconduct punishable by dismissal from employment. Besides dismissal from employment, inadvertent or negligent mishandling of taxpayer information may lead to disciplinary action including warnings, temporary suspension and demotion.

discourage breaches and violations.

Sanctions may be contained in tax, public administration, or criminal legislation, or a mix of all. What matters is that there is an appropriate consideration of administrative, civil and/or criminal penalties or sanctions, covering a broad range of violations of confidentiality or improper use of information.

The seriousness of sanctions (e.g. admonition, suspension of duties, financial penalty, or imprisonment) will usually depend upon the seriousness and impact of the conduct leading to their application.

Sanctions should be applicable to the various persons who may handle taxpayer information and commit a violation:

- Personnel, both permanent employees (e.g. career civil servants) and temporary employees (term contracts, time-limited appointments).

- External contractors, including legal and natural persons.

Sanctions should also cover violations committed by past personnel and contractors, i.e. after their duties with respect to taxpayer information cease. Box 43 provides an example of sanctions applied to unauthorised disclosure of taxpayer information.

SUB-REQUIREMENT 3.3.2: PROCESSES TO DEAL WITH SUSPECTED OR ACTUAL BREACHES OR OTHER NON COMPLIANCE, INCLUDING EFFECTIVELY APPLYING SANCTIONS

Sanction provisions should be supported by the necessary processes and resources to ensure their effective application. It is also necessary to have processes covering what happens upon the occurrence or suspicion of a breach, or of non-compliance with policies, up until when a decision is made to apply an appropriate sanction (or until the situation is otherwise resolved, without the need for a sanction).

When taxpayer confidentiality is violated, it may be the result of an unintentional act, deficiencies in the systems and procedures to protect the confidentiality of information, or it may be the result of intentional actions for the personal gain of one or more persons (for example due to corruption).

Whether it is the result of intentional or unintentional actions, any breach of confidentiality must be taken seriously and acted upon immediately. The appropriate actions to be taken will depend on the circumstances of the breach. If it is the result of an intentional act for personal gain, it would generally be appropriate to refer the matter to law enforcement officials for possible criminal charges.

Planning and preparing for confidentiality breaches in advance – i.e. having processes to manage them – enables jurisdictions to handle situations arising from breaches more promptly and effectively. An effective breach management system requires processes delineating the reporting, escalation, investigation and disciplinary procedures, and stakeholders' roles and responsibilities at each step. The processes should anticipate different breach scenarios of varying seriousness. The processes should be revised and improved as necessary, based on the experience applying them.

SR 3.3.2 requires four different types of processes to be in place with respect to breaches, including those that concern exchanged information, as depicted in Figure 21.

The Global Forum has prepared and can provide jurisdictions, upon request, more detailed guidance on good practices in data breach management and the requirements of SR 3.3.2.

Enforcement provisions and processes to address confidentiality breaches (Core Requirement 3.3)

SR 3.3.2.1. Processes when there is a suspected or actual breach, to ensure reporting and investigation

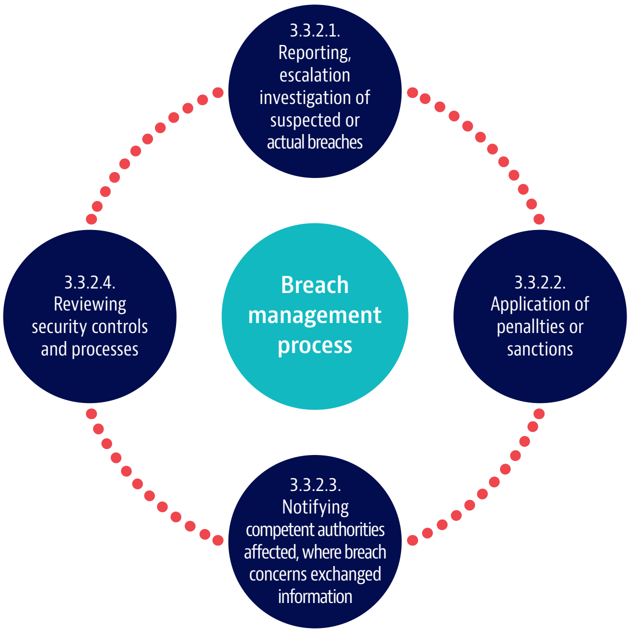
SR 3.3.2.1 requires jurisdictions to have processes to follow when there is suspected or actual unauthorised access, use or disclosure, which should ensure such issues are reported and investigated. These aspects are discussed in turn.

Reporting processes

Tax administrations' processes should provide for personnel to report suspected or actual breaches of confidential information, including exchanged information, and the steps for reporting, registering and escalating an incident. The processes should be documented and available to personnel for easy reference so that they know relevant chain of reporting or escalation. Training should also be provided. Often, a tax administration's security department is in charge of receiving the reports.

As an example, the processes could provide that personnel should report a suspected or actual breach of information in writing to the immediate line manager, or to a designated responsible official who, if necessary and depending on the seriousness of the incident, will escalate the matter to senior management, e.g. to the head of the tax administration.

FIGURE 21. **Main elements of managing confidentiality breaches**


3.3.2.1. Reporting, escalation investigation of suspected or actual breaches
Breach management process
3.3.2.2. Application of penallties or sanctions
3.3.2.3. Notifying competent authorities affected, where breach concerns exchanged information
3.3.2.4. Reviewing security controls and processes

The process may also envisage that the designated responsible official will first make preliminary inquiries with the reporting and reported persons and/or their managers, before deciding whether to formally trigger a breach management procedure, including a formal investigation.

The process may require reporting personnel to report all relevant knowledge or evidence in their possession that supports their suspicion or knowledge of a breach. The process may also provide for follow-up engagement with the reporting personnel, for any further information in respect of their report.

Investigation processes

If a reported incident requires an investigation, it should then be carried out and be broad enough to determine:

- The circumstances that led to the breach or violation.
- The person or persons responsible.
- Where possible, the cause of the breach.

Tax administrations' processes should therefore also cover the investigation and fact-finding procedures to examine the extent and seriousness of a reported breach. The investigation should not hold up any immediate steps that can be taken to minimise the impact of the breach, e.g. removing a suspected perpetrator's access to information systems or isolating the physical or IT environments in which compromised data was held.

Investigation processes will generally cover the following aspects:

- **Preliminary investigation to determine the seriousness of a breach**. The preliminary investigation may determine the type of breach (e.g. cyber attack, data theft by an insider, lost documents or storage media), the scale of the data breached (few data or a whole data set), the type of data involved (e.g. domestic taxpayer data, AEOI or EOIR data), or any exchange partner jurisdictions impacted.
- **Identification of the person(s) in charge of investigating and the internal and external stakeholders that should be involved**. The

official(s) in charge of overseeing and coordinating investigations should be clearly identified. Procedures could also set out what coordination between different departments will need to occur if an incident is sufficiently serious to require a comprehensive investigation (e.g. IT department, internal audit department, and the relevant business units such as the EOI unit). The necessary coordination with external stakeholders can also be set out (e.g. affected taxpayers, data providers, the data protection authority, the police, and foreign competent authorities, if the breach involves exchanged information). In very serious breaches, making a police report could be prescribed.

- **Evidence-gathering procedures**. Evidence is a key element of the investigative process, as it will help determine the person(s) responsible and inform the prevention of similar breaches in the future. Evidence will be essential for the proper application of sanctions, including criminal sanctions, if warranted. Clear procedures should therefore be in place for conducting inquiries and evidence-gathering, e.g. by audit or disciplinary departments, and in co-operation with law enforcement authorities, as appropriate.
- **Interim measures**. While investigations are pending, the procedures might enable appropriate administrative actions to be taken, such as transferring or suspending the person(s) suspected, or actually responsible, for the breach, in order to ensure fair and transparent investigations.

Following the investigation, a report should be prepared for management and include recommendations for any actions or sanctions to be taken against the person(s) responsible (law enforcement authorities may be involved in case of suspected intentional disclosure).

SR 3.3.2.2. Resources, processes and procedures to take remedial action and apply appropriate sanctions where issues are identified

Tax administrations' processes should also ensure the effective imposition of penalties or sanctions based on the legal framework, covered in SR 3.3.1.

SR 3.3.2.2 therefore states that jurisdictions should, with the support of adequate administrative resources, processes and procedures, ensure that remedial action is taken where actual issues have been identified, with appropriate penalties or sanctions applied in practice against employees, contractors and other persons who violate confidentiality rules, security policies or procedures, to deter others from engaging in similar violations.

The processes should describe the administrative steps for imposing disciplinary and administrative sanctions such as warning, suspension, demotion, salary reduction or dismissal, depending upon the gravity and seriousness of a breach.

There will usually exist an authority within the tax administration, or elsewhere within the public sector, responsible for applying administrative or disciplinary sanctions. Such authority will usually be conferred the necessary powers to impose the relevant sanctions, or to escalate matters to the police or other enforcement authority, as appropriate. The processes for transferring matters to the police for criminal investigation and prosecution should be documented. The relevant legal provisions that can be invoked for the application of administrative, civil or financial penalties, or for criminal referrals, may also be documented for ease of reference.

SR 3.3.2.3. Notifying foreign competent authorities of breaches of confidentiality of exchanged information

If a breach of confidentiality concerns exchanged information, an essential aspect of managing and responding to it is communicating with exchange partners.

Under international exchange agreements, jurisdictions are generally required to promptly inform the competent authorities of the exchange partners that provided the information disclosed or used in an unauthorised manner, so that they may formulate appropriate responses under their domestic legal framework and the applicable agreements.[21] Communications by the jurisdiction where a breach occurs are also important to give exchange partners assurance that the causes will be swiftly and thoroughly investigated, and that

[21] In the case of some multilateral agreements, the competent authority of the jurisdiction where a breach of exchanged information occurred must notify the Co-ordinating Body Secretariat of the agreement, which will in turn notify other competent authorities with respect to which a multilateral agreement is in effect to facilitate their information. See, for example the Common Reporting Standard (CRS) Multilateral Competent Authority Agreement (MCAA), section 5(2), and the MCAA on the exchange of country-by-country reports, section 5(3).

remedial action will be taken. These are key aspects of maintaining confidence in international tax information exchange.

SR 3.3.2.3 therefore requires jurisdictions to apply processes to notify other Competent Authorities of breaches of confidentiality or failure of safeguards, and of sanctions and remedial actions consequently imposed.

Notifications to foreign competent authorities would generally be expected to include the following aspects:

- Where the breach occurred (e.g. which organisation, which division or system of a tax administration).
- The type of breach (e.g. cyber-attack, data theft by an insider, lost documents or storage media).
- The type of data involved (e.g. EOIR file, or AEOI data).
- Actions being taken to contain, eradicate and analyse the situation.
- Central point of contact in the tax administration and other relevant contact points.

After the initial notification, it may be appropriate for a tax administration to continue to communicate with the concerned exchange partner(s) to better enable them to take appropriate actions within their jurisdiction (such as fulfilling any domestic legal obligations to notify affected taxpayers and data protection authorities). In some cases it may be appropriate to issue public communications.

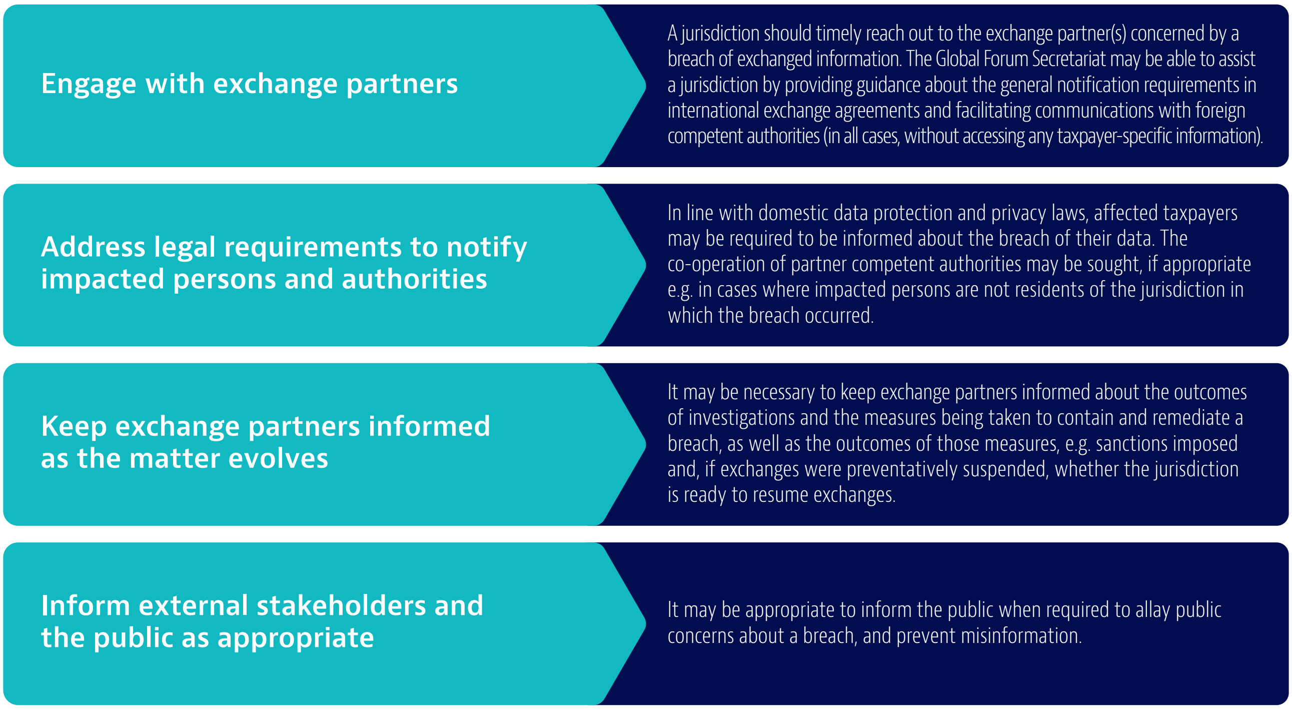
Figure 22 depicts the possible communication steps involved where a breach of exchanged information occurs.

SR 3.3.2.4 Review of security controls, monitoring and enforcement processes in response to non-compliance

It is essential to learn from incidents and breaches, in order to continuously improve the processes and controls aimed at monitoring, preventing and handling future ones.

SR 3.3.2.4 therefore provides that jurisdictions should review the monitoring and enforcement processes in response to non-compliance, with senior management ensuring that recommendations for change are implemented in practice.

FIGURE 22. **General communications steps in case of a breach concerning exchanged information**



Engage with exchange partners

A jurisdiction should timely reach out to the exchange partner(s) concerned by a breach of exchanged information. The Global Forum Secretariat may be able to assist a jurisdiction by providing guidance about the general notification requirements in international exchange agreements and facilitating communications with foreign competent authorities (in all cases, without accessing any taxpayer-specific information).

Address legal requirements to notify impacted persons and authorities

In line with domestic data protection and privacy laws, affected taxpayers may be required to be informed about the breach of their data. The co-operation of partner competent authorities may be sought, if appropriate e.g. in cases where impacted persons are not residents of the jurisdiction in which the breach occurred.

Keep exchange partners informed as the matter evolves

It may be necessary to keep exchange partners informed about the outcomes of investigations and the measures being taken to contain and remediate a breach, as well as the outcomes of those measures, e.g. sanctions imposed and, if exchanges were preventatively suspended, whether the jurisdiction is ready to resume exchanges.

Inform external stakeholders and the public as appropriate

It may be appropriate to inform the public when required to allay public concerns about a breach, and prevent misinformation.

This means that tax administrations should generally review their breach monitoring, enforcement and management process, and relevant security controls, not only as a matter of routine as discussed in SR 3.2.6 about operations management, but also based on lessons learned from specific breaches.

To support these reviews, the reports prepared at the conclusion of a breach investigation may recommend, in addition to an appropriate sanction against the person(s) responsible:

- Measures to minimise the repercussions of the breach.
- Future actions to avoid similar breaches or incidents.
- Possible improvements (if necessary) to the reporting, investigation, disciplinary or administrative processes to apply sanctions.

Specific incident learnings should also feed into periodic (e.g. annual or biannual) reviews aimed at:

- Identifying longer term strategies to further mitigate the likelihood of breaches reoccurring.
- Enhancing the breach management process.

The investigating authority, the persons in charge of information security and confidentiality in the tax administration (e.g. ISO), and/or senior management, should then be responsible for following up to ensure that the improvement recommendations arising from a specific breach or a review of processes are implemented.

The review of security controls, monitoring or enforcement processes might result in:

- The implementation of corrective measures for the process where the breached occurred.
- The review of processes for the recruitment or engagement of personnel (employees and external contractors).
- The implementation of periodic training programs for the secure handling of confidential data and the promotion of security awareness.
- The review and improvement of ISM controls, e.g. access rights.
- The carrying out of more frequent data breach response drills.

See Box 44 for an example of a process to deal with breaches of confidential information.

Box 44. **Summary of a sample breach management policy**

Under the Jurisdiction B tax administration's Policy for the Reporting of Confidentiality Breaches and Security Incidents, all personnel and external contractors are required to report, in writing, to the Information Security Officer (ISO) actual or suspected breaches of confidentiality or incidents of violation of information security policies. The Policy establishes the roles and responsibilities of different personnel throughout the reporting and investigation.

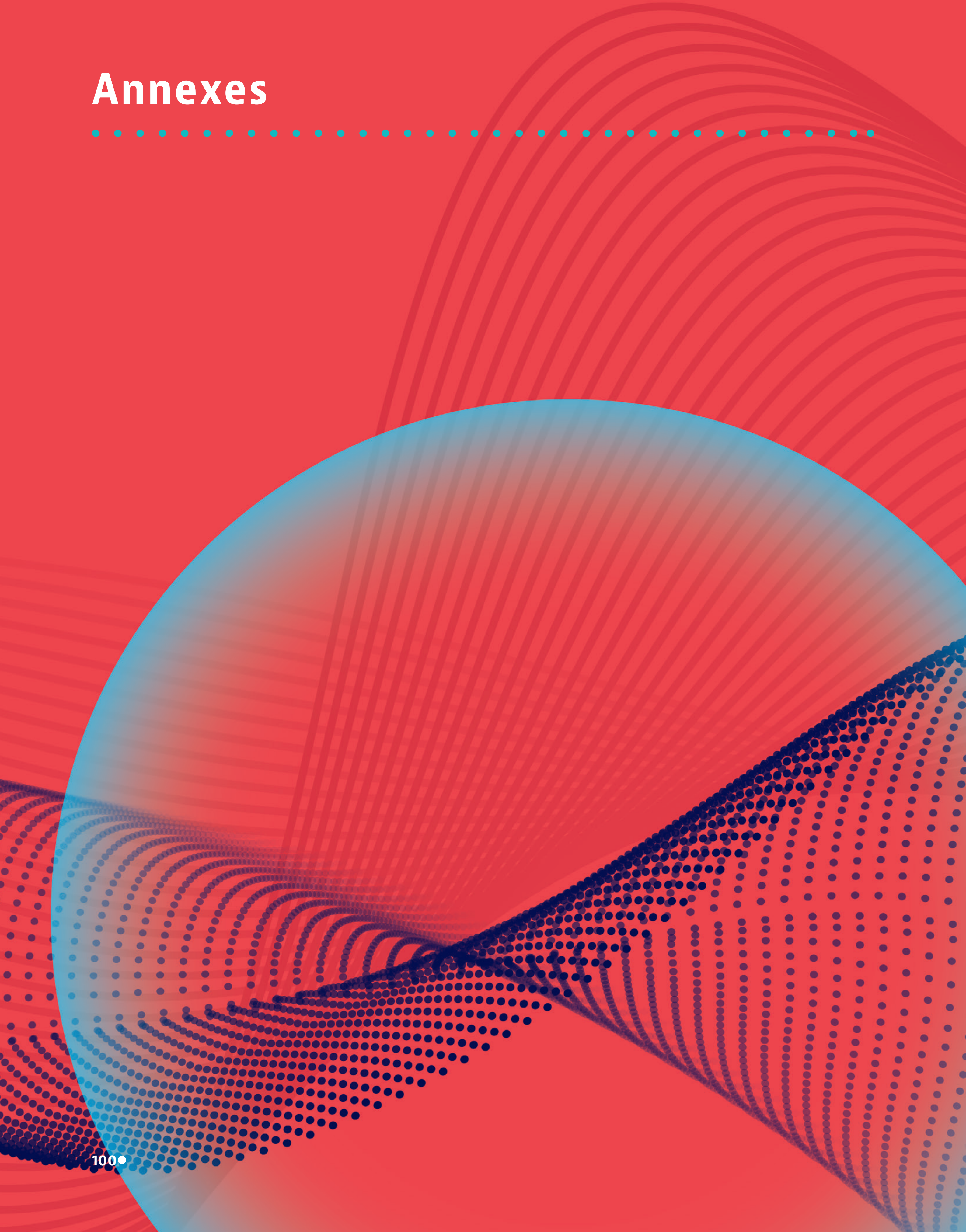
At the conclusion of the investigation, the line manager of the business process affected must elaborate a report, on the advice of the ISO, with an account of the incident, an assessment of its seriousness, and its probable causes. Depending on the nature, scale and seriousness of the incident, the line manager may decide to escalate the incident to the Information Protection Agency and/or refer the incident to the police.

Under the Policy, remedial measures must be applied to correct the failure that caused the breach. If the breach involves exchanged information, the incident must also be reported to the relevant exchange partner(s) and, where relevant, the Co-ordinating Body Secretariat of the applicable multilateral exchange agreement.

The line manager's report must recommend appropriate disciplinary actions to be taken against the responsible person(s). These can cover warning, dismissal, suspension, demotion and salary cut.

After the incident has been remediated and the investigation has finished, the ISO must prepare a report for the board of the tax administration indicating whether measures are recommended to improve any relevant policies, processes or security controls.

Annexes



Annex A. Glossary of concepts

CONCEPT	DESCRIPTION	SR
Acceptable use policy	Set of rules that establish the permitted and prohibited practices in relation to information systems that contain confidential information.	**3.2.5**
Access controls	Security controls that ensure that access to information, physical premises and systems is based on need to know and minimum rights.	**3.2.3**
Access management	Policies, processes and procedures, owned by senior management and not solely by the tax administration's IT function, that govern physical and logical access, and effective processes for the provisioning and auditing of logical access and for the identification and authentication of users.	**3.2.3**
Access provisioning	Effectively granting access to information through the creation of user accounts, password management, and by assigning specific access rights and authorisations to users.	**3.2.3**
Asset	Anything of value that is involved in the realisation of processes and the generation of results. Assets can be information, people, services, equipment, systems etc.	**3.2.1**
Asset management	Process that ensures that the tax administration's assets are identified and tracked from their creation/procurement to their destruction/disposal.	**3.2.4**
Audit function	Comprehensive, unbiased reviews to assess compliance with ISM system processes established in policies and procedures. Audit findings and results should be directly reported to the head of the tax administration.	**3.2.6**
Authentication	When a user accesses IT systems, the authentication process ensures and confirms a user's identity in a non-repudiation based manner.	**3.2.3**
Authorisation	Once a user is authenticated on a system, the user is then authorized to access resources based on need to now and least privilege principles.	**3.2.3**
Awareness	Awareness is about employees being regularly exposed to security messages alerting them of IT threats/risks or other security threats/risks, usually communicated to all employees at the same time, whether that be personnel in a particular work area or across the whole breadth of the tax administration, even including external third parties, etc.	**3.2.2**

CONCEPT	DESCRIPTION	SR
Baseline controls	Set of minimum security controls that a tax administration applies to certain risks, regardless of their severity.	**3.2.4**
Business continuity management	A management process to ensure the continuity of operations in the scenario of some event that disrupts normal operations.	**3.2.1**
Change management	Refers to the controlled management of the development of new systems and services, and making major changes to existing ones.	**3.2.6**
Classification of information	Process of identifying the types of information tax administrations hold and determining the level of protection they should receive.	**3.2.5**
Clean/clear desk policy	A clean/clear desk policy (CDP) specifies how employees should leave their working space when they leave their desks or the office, to ensure the confidentiality of information.	**3.2.5**
Competent authority	Competent authority(ies) is/are the person(s) or government authority(ies) designated by a jurisdiction as being competent to exchange information pursuant to any international exchange agreement.	**3.1.1,** **3.2.5**
Controls	See Practices.	**3.2.1**
Encryption	Encryption is a protection mechanism applied to the data making it accessible only if the proper decryption key is provided.	**3.2.5**
Firewall	Equipment placed on strategic points of a network (usually those facing external or internet access and internal separated zones) that allow or block traffic based on rules.	**3.2.4**
Identification	A process used in IT systems to uniquely identify the users who have an access right.	**3.2.3**
Incident management	Entails identifying, documenting and managing security incidents, both in the IT and non-IT areas.	**3.2.6**
Information security	Refers to the protection of the confidentiality, integrity and availability of information.	**3.2.1**
Information security risk	Potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation.	**3.2.1**

CONCEPT	DESCRIPTION	SR
ISM framework	An ISM framework refers to the organisational structures and overarching information security principles, aimed at guiding tax administrations to achieve ISM objectives, following a risk-based approach. The ultimate accountability for the ISM framework should sit with the most senior officials within the tax administration.	**3.2.1**
ISM policy	An ISM policy expresses the intent of the tax administration as to how it approaches information security. The ISM policy should set out the scope of the ISM system, and the general information security management objectives to which all other individual policies should adhere.	**3.2.1**
ISM system	An ISM system comprises the domain-specific policies, procedures and controls to implement the ISM framework. The ultimate accountability for the ISM system should sit with the most senior security officials within a tax administration.	**3.2.1**
IT security control	Administrative, technical or physical measure implemented to mitigate an IT risk	**3.2.4**
Least privilege	Access management principle that establishes that legitimate access should be restricted to the minimum specific functions that the users need to do their job.	**3.2.3**
Legitimate user	User who gets a specific access right based on the need to know and least privilege principles.	**3.2.3**
Log	A log, in a computing context, is the automatically produced and time-stamped documentation of events relevant to a particular IT system. Manual logs can be created for non-IT activities as well.	**3.2.6**
Log management	Refers to the collective processes and policies used to administer and facilitate the generation, transmission, analysis, storage, archiving and ultimate disposal of the large volumes of log data created within an IT system.	**3.2.6**
Logging	Logging refers to tax administrations recording and keeping track of all access to protected data, including access to facilities and areas where the data is held, and in particular to systems that hold taxpayers' records and other sensitive information.	**3.2.6**
Logical access	An access to systems through identification, authentication and authorisation processes.	**3.2.3**
Malware	Malicious software. Program created to exploit a vulnerability in a targeted system in order to harm it or steal information.	**3.2.4**
Media sanitisation	Sanitisation is the process of treating data held on storage media to reduce the likelihood of retrieval and reconstruction to an acceptable level.	**3.2.5**

CONCEPT	DESCRIPTION	SR
Naming conventions	Refers to rules on how information is named to clearly identify it from other.	**3.2.1**
Need to Know	Access management principle that establishes that taxpayer information should only be accessed by personnel with a legitimate business reason to do so.	**3.2.3**
Non-disclosure agreement	Formal statements or contracts defining the rules for the non-disclosure of confidential information to third parties.	**3.2.2**
Outsourcing	Recourse to an external provider for the provision of goods and services.	**3.2.4**
Penetration testing	Penetration testing effectively simulates the actions of a hacker against the organisation	**3.2.4, 3.2.5**
Phishing	Type of online scam where criminals send out fraudulent email messages that appear to come from a legitimate source and trick the recipient into sending confidential information such as credentials for access to systems.	**3.2.2**
Physical access	An on-site access to specific areas.	**3.2.3**
Policy	A policy is a documented statement of the tax administration to implement processes, procedures and controls in a given area. A policy answers the question "what should be done?" There should be a hierarchy of policies. For example, a policy on identification and authentication for access to IT systems will be subsidiary to an overall policy on Access Management. There should also be an overarching Information Security Management Policy that enumerates the overarching security principles that apply to all policies.	**3.2.1**
Practices or Controls	A control or practice is a specific measure that is used to manage information security risk (i.e. mitigate or eliminate a risk). Controls can include process and procedures, as well as programs, tools, techniques, technologies and devices. Controls are sometimes also referred to as safeguards or countermeasures for an identified risk.	**3.2.1**
Procedure	A procedure is a documented set of steps and activities to implement security policies. A procedure answers the question "how should it be done and by whom?" The term procedure is often linked to the term process – processes and procedures – because a procedure is usually a more detailed representation for each step of a process. There may often be more than one procedure for each step of a process. For example, a process may concern the submission of a tax return, but there may be different ways in which submission can be executed, and therefore different procedures for each method of submission.	**3.2.1**

CONCEPT	DESCRIPTION	SR
Process	A process is a repeatable sequence of actions with a measurable outcome. The concept of processes is critical to ISM. Measuring outcomes and acting on results is the foundation for improving processes and security. A process can be anything from a tax business process such as the submission and assessment of tax returns to the process for updating IT software. Any action that is not covered by a defined process is by definition a security risk, since there is no assurance of repeatability, and measuring and improving outcomes.	**3.2.1**
Recovery	Refers to restoring services and business operations in case of high failure.	**3.2.4**
Resilience	Refers to mitigating the risk of service interruption and ensuring tolerance to failures in services by providing continuity of service up to a certain point.	**3.2.4**
Retention period	Statutory requirement to retain information for a fixed period even if the information is no longer need for tax business purposes.	**3.2.5**
Risk mitigation	Refers to actively implementing measures to lower the impact or the probability of occurrence of a risk.	**3.2.1**
Security Operations Centre	A Security Operations Centre is a team of specialised professionals and systems for monitoring and analysing the security posture of the tax administration on an ongoing basis	**3.2.6**
Service Level Agreement	Agreement that sets the minimum level of service an entity providing a service must comply with.	**3.2.4**
Social engineering	It refers to maliciously exploiting the trusting nature of personnel to obtain information that can be used for personal gain. This activity is also known as "people hacking".	**3.2.2**
Supplier management	Risk-based process that ensures that an external supplier accessing a tax administration's data or premises does not put at risk confidentiality and security.	**3.2.4**
Training	Training is about tax administration personnel (employees/contractors) acquiring and developing the knowledge, skills and core competences needed to integrate confidentiality and security into tax processes.	**3.2.2**
Vulnerability	Flaw in the design of an asset or its nature.	**3.2.1,** **3.2.6**
Vulnerability management	Refers to the processes and procedures for the identification and management of vulnerabilities.	**3.2.6**

Note: There may be official definitions of these concepts from relevant referent sources, but these are the definitions that we use for the purposes of the ISM toolkit.

Annex B. Useful resources

Relevant information on international standards on tax transparency and exchange of information

- Model Competent Authority Agreement within the Automatic Exchange of Information Standard: https://www.oecd.org/tax/exchange-of-tax-information/standard-for-automatic-exchange-of-financial-account-information-in-tax-matters-second-edition-9789264267992-en.htm

- Standard for Exchange of Information on Request: http://www.oecd.org/tax/transparency/documents/global-forum-handbook-2016.pdf

- Global Forum's Plan of Action for Developing Countries' Participation in AEOI: https://www.oecd.org/tax/transparency/documents/plan-of-action-AEOI-and-developing-countries.pdf

- Terms of Reference for the Automatic Exchange of Information peer review process: https://www.oecd.org/tax/transparency/documents/AEOI-terms-of-reference.pdf

- Global Forum on Transparency and Exchange of Information for Tax Purposes: http://www.oecd.org/tax/transparency/

- Exchange of Information on Request: http://www.oecd.org/tax/transparency/what-we-do/exchange-of-information-on-request/exchange-of-information-on-request-peer-review-process.htm

- Automatic Exchange of Information: http://www.oecd.org/tax/automatic-exchange/

  https://read.oecd-ilibrary.org/taxation/standard-for-automatic-exchange-of-financial-account-information-in-tax-matters-second-edition_9789264267992-en

- Common Reporting Standard: https://www.oecd.org/tax/automatic-exchange/common-reporting-standard/

- Technical assistance available from the Global Forum on Transparency and Exchange of Information for Tax Purposes: https://www.oecd.org/tax/transparency/what-we-do/

- OECD Guide on the Protection of Confidentiality of Information Exchanged for Tax Purposes: https://www.oecd.org/ctp/exchange-of-tax-information/keeping-it-safe-report.pdf

Model international exchange agreements

- OECD Model Tax Convention on Income and on Capital: https://read.oecd-ilibrary.org/taxation/model-tax-convention-on-income-and-on-capital-condensed-version-2017_mtc_cond-2017-en

- OECD Model Agreement on Exchange of Information in Tax Matters: https://www.oecd.org/tax/exchange-of-tax-information/2082215.pdf

- United Nations Model Tax Convention Between Developed and Developing Countries: https://www.un-ilibrary.org/content/books/9789210474047

- Convention on Mutual Administrative Assistance in Tax Matters: https://read.oecd-ilibrary.org/taxation/the-multilateral-convention-on-mutual-administrative-assistance-in-tax-matters_9789264115606-en

OECD
BETTER POLICIES FOR BETTER LIVES

For more information:

www.oecd.org/tax/transparency

gftaxcooperation@oecd.org

@OECDtax | #TaxTransparency