cooperación
alemana
DEUTSCHE ZUSAMMENARBEIT

Implemented by:

giz Deutsche Gesellschaft
für Internationale
Zusammenarbeit (GIZ) GmbH

Guide for the Protection and Ethical use of Information Held by Tax Administrations.

Tax Administrations of Central America, Panama and the Dominican Republic

In coordination with:

COSEFIN
Consejo de Ministros de Hacienda o Finanzas de Centroamérica, Panamá y República Dominicana

SICA
Sistema de la Integración Centroamericana

CENTRO INTERAMERICANO DE ADMINISTRACIONES TRIBUTARIAS
CIAT
FUNDADO 1967

Guide for the Protection and Ethical use of Information Held by Tax Administrations

cooperación
alemana
DEUTSCHE ZUSAMMENARBEIT

Implemented by:

giz Deutsche Gesellschaft
für Internationale
Zusammenarbeit (GIZ) GmbH

In coordination with:

COSEFIN
Consejo de Ministros de Hacienda o Finanzas de
Centroamérica, Panamá y República Dominicana

SICA
Sistema de la Integración
Centroamericana

CIAT

Guide for the protection and ethical use of information held by the tax administrations. Tax Administrations of Central America, Panama and the Dominican Republic
ISBN: 978-9962-722-82-3

Published by:

Inter-American Center for Tax Administrations – CIAT
Ramón Arias Avenue, Panama City, Panama
Tel. (+507) 307 CIAT (2428)
www.ciat.org

Deutsche Gesellschaft für

Internationale Zusammenarbeit (GIZ) GmbH

Company's offices

"Good Financial Governance Program" Agency GIZ, Order of Malta Boulevard,
German Cooperation House, Santa Elena Urbanization
Old Cuscatlán, La Libertad El Salvador, Central America.
Tel. +503 2121 5100
Giz-el-salvador@giz.de
Zentralamerika – giz.de

English Version

July (2025)

Commissioned by the:

Federal Ministry for Economic Cooperation and Development (BMZ) of Germany

Intellectual Property Rights

The opinions expressed and arguments used in this publication do not necessarily represent the official views of the Inter-American Center of Tax Administrations (CIAT), its member countries, the German Development Cooperation, GIZ, or the German Federal Ministry for Economic Cooperation and Development, BMZ. For official information, please visit www.ciat.org or the official GIZ website.

Authors

Alfredo F. Revilak De la Vega
Ana Y. Rodríguez Calderón
A. Gabriela Contreras Delgado
Evelyn Molina Bolaños

Reviewed by:

GIZ

Gustavo Ernesto Sánchez Buriticá
Orlando Castellón Tellería
Manfredo Octavio Chocano Alvarado

CIAT

Raul Zambrano
Mónica Alonso
Elizabeth Rodríguez

Contents

Authors[1]

Alfredo F. Revilak De la Vega, is an independent consultant with over 30 years of experience in the commercial and public sectors, including positions at Citibank, BBVA and the Mexican Ministry of Finance and Public Credit, specifically in the Financial Intelligence Unit and the Tax Administration Service. His experience includes 10 years as a specialist evaluator and consultant in information protection and data safeguarding (OECD and World Bank) in Tax Administrations, participating in the evaluations and technical support of: Panama, Costa Rica, Belize, St. Kitts and Nevis, Trinidad and Tobago, Mexico, Chile, Argentina, Peru, Ecuador, Colombia, Uruguay and Paraguay. He currently spends most of his time as Senior International Tax Consultant in the Fiscal Policy and Sustainable Growth Unit of the World Bank's Macroeconomics, Trade and Investment Global Practice.

Ana Y. Rodríguez Calderón, has more than 15 years of experience in international taxation, and has dedicated her career to international taxation, cooperation and development issues. She worked for 4 years at the Costa Rican Ministry of Finance, where she held a number of positions, including Head of the Minister's Office, Director of International Affairs and Advisor to the Minister on international taxation issues. Ana worked for more than 7 years at the OECD as a policy analyst and later as an advisor coordinating the Global Tax Relations Program (GRP). Currently, Ana is an international consultant and works mainly as a Senior International Tax Consultant for the World Bank and the Asian Development Bank. She has also provided her services to the IDB, CIAT, IBFD and the United Nations.

A. Gabriela Contreras Delgado, is a lawyer specializing in tax law. She collaborated in the Mexican Tax Administration Service for 15 years where she participated in the regulatory implementation of the automatic exchange of financial information agreements. She has been a representative of the Mexican delegation before the OECD, the Global Forum and the IRS and served as competent authority in the negotiation and attention of several Mutual Agreement Procedures with competent authorities of other jurisdictions. She is currently an independent consultant and has provided her services in the private sector, as well as to various tax authorities, the World Bank and CIAT, among others.

Evelyn Molina Bolaños, is an economist and data scientist with more than 10 years of experience in regional digital development programs. She worked for 3 years at the Costa Rican Ministry of Finance, where she

[1] The authors would like to express their sincere gratitude to the officials of the tax administrations of Costa Rica, El Salvador, Guatemala, Honduras, Dominican Republic and Panama for their valuable collaboration in the development of this guide.

served as an economic advisor to the minister. In 2015 Evelyn joined the Citizen Service Innovation Division of the Inter-American Development Bank (IDB) in Washington DC, where she led and supported in regional data governance programs. Evelyn is currently an independent consultant and has provided her services to different development agencies, including CIAT and the IDB.

1. Introduction

Within the framework of the cooperation agreement between the Inter-American Center of Tax Administrations (CIAT) and the German Development Cooperation (GIZ) to strengthen the capacities of the Tax Administrations of Central America, Panama and the Dominican Republic, CIAT has been entrusted with the preparation of a Guide for the protection of information held by the tax administrations that provides recommendations on how to approach a strategy aimed at adequate data protection

Personal data protection plays a crucial role in tax administrations by safeguarding the integrity and confidentiality of tax data. Tax information, by its nature, requires robust safeguards to prevent unauthorized access, alteration or improper disclosure that could compromise taxpayers' privacy. In addition, public confidence and the credibility of the tax administration depend to a large extent on the security of the information managed. The effective implementation of protection measures not only safeguards tax information against internal and external threats, but also contributes to the legitimacy and transparency of tax operations, thus strengthening the relationship between the tax administration and taxpayers.

Thus, the main objective of this guide is to provide tax administrations with recommendations on how to approach a strategy aimed at adequate data protection, including procedural aspects and those related to information security. Specifically on the topics of (i) legal framework, (ii) information protection management, (iii) information technology security management, (iv) monitoring and prevention, (v) generation of open data in the tax administrations, (vi) data governance in the tax administrations and (vii) use of the cloud.

2. Methodology for the Preparation of the Guide

This guide was developed based on a comprehensive approach that combined a literature review and the collaboration of subject matter experts. The key steps of the methodology used are detailed below:

1. **Research and document review:** international best practices and case studies relevant to tax administrations on data protection issues were identified. This process included a review of existing tax legislation, as well as manuals, regulatory guides and publications of international organizations with expertise in the field**.**

2. **Data collection and comparative analysis:** Data was collected and analyzed on data protection procedures and policies in the tax administrations of Costa Rica, El Salvador, Guatemala, Honduras, Dominican Republic and Panama. This comparative analysis made it possible to identify useful recommendations to be adapted to the specific contexts of the countries involved.

3. **Consulting and interviews with experts:** experts in technology, information security management, lawyers and others from the tax administrations of Costa Rica, El Salvador, Guatemala, Honduras, Dominican Republic and Panama were consulted. The interviews and consultations provided valuable insights into local practices and country-specific needs**.**

4. **Identification of case studies:** based on the feedback received, practical examples and relevant case studies were included to provide further clarity on best practices**.**

5. **Review and validation:** once the draft guide was completed, a review was carried out with CIAT and country counterparts to ensure accuracy and consistency of content.

3. Legal Framework

3.1. Introduction

Taxpayers' rights are fundamental to any democratic and just society. These rights ensure that citizens who comply with their tax obligations are treated fairly and transparently by the tax authorities. The importance of these rights lies in the preservation of trust in the tax system, which consequently promotes citizens' participation in financing the State.

Therefore, transparency and access to information are fundamental pillars of an effective and ethical tax administration. The proper use of information held by tax administrations facilitates accountability, combats tax evasion and promotes an equitable distribution of the tax burden. However, this access must be regulated to safeguard the privacy and rights of taxpayers, thus maintaining a balance between access to information and the protection of privacy and confidentiality of data. This is why safeguarding the confidentiality of information is the third fundamental principle of tax management that is essential to promote confidence in the tax system.

In this context, this chapter will address relevant aspects related to taxpayers' rights and guarantees regarding the information that the tax administration has on them, highlighting the need for a legal framework that ensures fair and equitable treatment. The characteristics of the legal provisions focused on guaranteeing transparency in tax administration while safeguarding individual rights and protecting sensitive information will be examined. It will also analyze the legal framework necessary to ensure a balance between these elements at both the national and international levels.

Furthermore, the mechanisms designed to safeguard the confidentiality of tax data and information will be explored, recognizing the importance of protecting taxpayers' privacy. Finally, the main characteristics of the regulatory sanctioning framework through which the authorities seek to prevent, reduce and dissuade the recurrence of infractions related to confidentiality and data security, improper use and disclosure of information, and transparency infringements, will be reviewed.

To enrich this analysis, references to the regulatory frameworks of Costa Rica, Guatemala, Honduras, El Salvador, Panama, Dominican Republic, and other jurisdictions are included in order to identify the different strategies and approaches adopted globally and to highlight measures and best practices that favor data protection without undermining fiscal transparency, thus contributing to strengthen fiscal systems globally.

3.2. Taxpayer Rights and Guarantees

Fundamental Rights and Guarantees

The United Nations (UN) defines **human rights** as those “inherent to all human beings, regardless of race, sex, nationality, ethnicity, language, religion or any other status (..) without discrimination.”[2] These rights include, among others, the right to life, freedom, work, education and freedom of expression. These rights are qualified as universal because they refer to any individual, are independent, interrelated and indivisible. In light of these rights,governments are obliged to act in certain ways or to refrain from certain acts in order to ensure their protection and preservation.

In addition, **fundamental rights** are “those that are positivized in the legal system, in such a way that their basis is the legal norm, so that their source is the will of the competent authority to create such norms. They produce legal effects, whether rights or obligations and even rights of action, and have all the legal consequences attributed to them by the legal system. They exist from the moment they are granted by the legal system, and are ensured by the means of control of their exercise that it establishes as a guarantee against abuses by the authority. Their limits are found in the law itself. (...) Constitutional law is responsible for regulating the protection of fundamental rights and for providing special mechanisms for their protection.”[3]

In general, both human rights and fundamental rights have essential attributes that characterize them; these are:

a) Universality: This refers to the scope of the protection provided by the right; ideally, it is intended to cover, if not all, the greatest number of rights holders and the conditions protected by them.

b) Interdependence and Indivisibility: Interdependent as they are interrelated and indivisible as they must be observed as a whole; the deprivation of one right negatively affects the rest of them. They cannot be protected or safeguarded in isolation but as a single legal body.

c) Progressivity: They are progressive because they satisfy the needs of the individual at each particular historical moment; they are not static rights, but have gradually increased according to social progress or advancement.

[2] United Nations. *Human rights*. https://www.un.org/en/global-issues/human-rights

[3] Huerta, Carla, *Sobre la distinción entre derechos fundamentales*. Inter-American Court of Human Rights. Article available at: https://www.corteidh.or.cr/tablas/r28772.pdf

Based on the foregoing, it can be concluded that fundamental rights are set forth in a legal norm or body of law, which gives them legal effects (rights or obligations) and the State has the obligation to safeguard them by making use of the means of control available to it, within the scope of its powers. The rights and guarantees of taxpayers can be included in this category since they are rights that are set forth in a body of law and the State has the obligation to preserve them by using the means of control at its disposal, within the scope of its powers.

Background Information on Taxpayers' Rights

Now, in the fiscal context, the first formal precedent at the international level where fundamental rights were protected was the **Declaration of the Rights of Man and of the Citizen** [4] which established the obligatory nature of contributions to cover government expenditures in accordance with the *principles of generality and proportionality*.

Subsequently, the **Declaration of Human Rights** [5] it also set forth rights that, although not exclusive to taxpayers, constitute a precedent of the rights that are currently recognized in the tax context. Among the main rights enshrined therein are: the right to security, equality before the law, judicial protection, the right to a hearing and the right and protection of individual and collective property.

Likewise, the **American Convention on Human Rights** (colloquially known as the Pact of San José) [6]) also collected various fundamental rights from the instruments mentioned above, but emphasizes the right to due process when filing appeals before independent and impartial courts that allow access to protection against acts that could violate their fundamental rights. These rights are currently recognized as judicial guarantees that have an effect in criminal, civil, labor, and even tax matters, indicating that jurisdictional protection extends to tax obligations.

[4] Adopted by the French National Constituent Assembly on August 26, 1789. Document available at https://www.conseil-constitutionnel.fr/sites/default/files/as/root/bank_mm/espagnol/es_ddhc.pdf

[5] Declared by the United Nations' General Assembly in Paris, on December 10, 1948 in resolution 217-A. Information available at https://www.un.org/es/about-us/universal-declaration-of-human-rights

[6] Signed on November 22, 1969. Complete document available at https://www.oas.org/dil/esp/1969_Convenci%C3%B3n_Americana_sobre_Derechos_Humanos.pdf

Fundamental rights and guarantees of taxpayers

In 1990, the OECD, through the Committee on Fiscal Affairs, published a survey[7] that analyzed the legal status of taxpayers' rights and obligations among its member countries. This survey is one of the first comparative analyses of the fundamental rights and guarantees of citizens in the field of taxation.

Based on the information received in this survey, the OECD identified the rights, guarantees and obligations that were most recurrent in the legislation of the countries evaluated. These results are summarized below:

Taxpayers' Rights and Guarantees	Taxpayers' Obligations
The right to be informed, assisted and heard.	The obligation of being honest when complying with fiscal obligations.
The right to appeal.	The obligation of cooperating with fiscal authorities.
The right to pay no more than the correct amount of taxes.	
The right of legal certainty.	The obligation of providing information and documents punctually and adequately.
The right to privacy.	The obligation of keeping registries, accounting and files.
The right to confidentiality and secrecy.	The obligation to pay taxes in due time and form.

Source: Taxpayers' rights, guarantees and obligations – OECD Survey 1990

In addition, the OECD study identified the different approaches adopted by jurisdictions to translate such rights and guarantees into their regulations:

a) **Taxpayers' Bill of Rights**: Some jurisdictions concentrated the measures taken to protect taxpayers in a letter or general statement of general principles that should govern the relationship between the tax authorities and the taxpayer. Such is the case of the United States[8] or Canada[9] that have a Taxpayer Bill of Rights. In other countries, these documents provide a more detailed guide to taxpayers' rights focused on

[7] OECD, Taxpayer's Rights and Obligations – Practice Note. Full document available at: https://www.oecd.org/ tax/administration/Taxpayers'_Rights_and_Obligations-Practice_Note.pdf

[8] Document available at https://www.irs.gov/es/taxpayer-bill-of-rights

[9] Document available at https://www.canada.ca/en/revenue-agency/corporate/about-canada-revenue-agency-cra/taxpayer-bill-rights.html

some of the phases of the evaluation process, such as the Bill of Rights of the Audited Taxpayer[10], in the case of Mexico, or Honduras and the Bill of Rights and Obligations of the TO in Audit Actions[11].

b) **Inclusion in tax administration returns:** Where some jurisdictions chose to include indications on the expected behaviors of officials and taxpayers as part of the mission of the tax administrations. Such is the case of the United Kingdom[12], whereas the document known as the HMRC Charter defines the service and standard of behavior that clients should expect when interacting with the tax administration of that jurisdiction.

c) **Tacit recognition through other tax provisions:** Some jurisdictions do not have an express declaration that indicates the rights of taxpayers, however, in their tax provisions there is a recognition by the tax authority with respect to rights similar or comparable to the rights and guarantees of taxpayers. An example of this approach is found in Costa Rican legislation, which in its Code of Tax Rules and Procedures[13] includes a chapter focused on taxpayer rights and guarantees.

   Although the OECD study referred to above does not expressly indicate this, it would be appropriate to add an additional category to those previously indicated:

d) **Elevation to the rank of law:** There are jurisdictions in which the recognition of the taxpayers' basic rights and guarantees in their relationship with the tax authorities is set forth in a Law in order to guarantee legal protection and certainty at the highest possible regulatory level; such an approach is the one adopted by Mexico with the Federal Law of Taxpayers' Rights[14].

Regardless of the approach taken, it is valid to note that the main rights and fundamental guarantees of taxpayers could be classified into the following categories based on the protected rights or the scope of application:

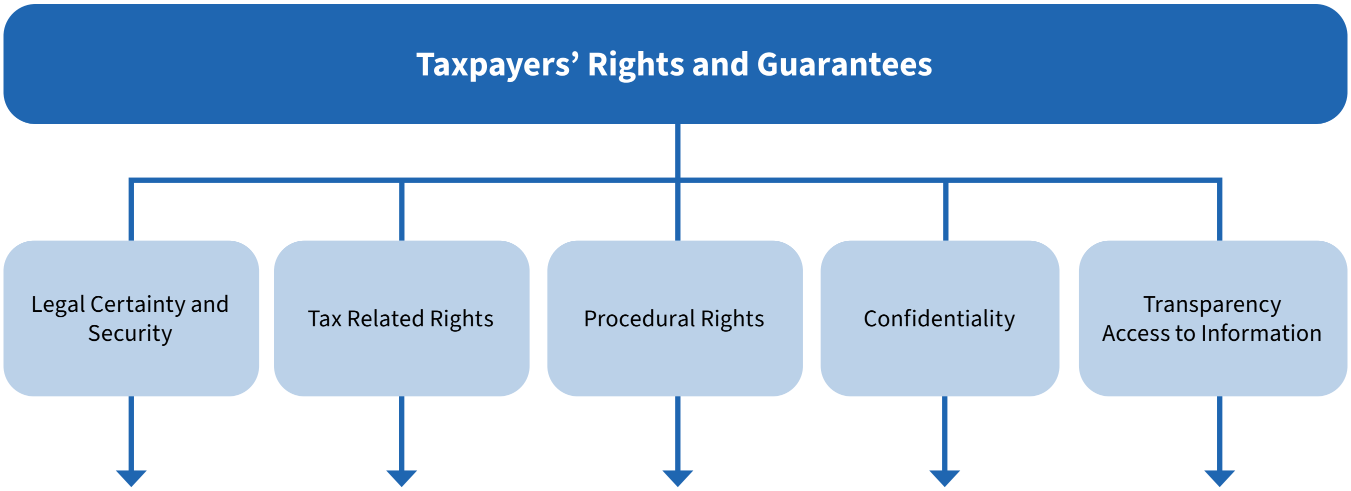
[10] Document available at http://omawww.sat.gob.mx/informacion_fiscal/derechos_contribuyentes/Documents/Carta_Contr_Aud_072014.pdf

[11] Document available at https://www.sar.gob.hn/derechos-y-obligaciones/

[12] Complementary information available at https://www.gov.uk/government/publications/hmrc-charter/the-hmrc-charter

[13] Complete text available at: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_articulo.aspx?param1=NRA&nValor1=1&nValor2=73336&nValor3=89973&nValor5=3

[14] Complete text available at: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFDC.pdf



Taxpayers' Rights and Guarantees

Legal Certainty and Security

- Right to consistent application of the law
- Non-discrimination.
- Right to be treated equally.
- Right to petition.
- Right not to be audited more than once for the same tax in the same period.

Tax Related Rights

- Right to the correct determination of contributions.
- Right to receive the appropriate tax refunds.
- Right to presumption of compliance.

Procedural Rights

- Right to appeal decisions made by tax authorities.
- Right to protection of sensitive and confidential information.
- Right to legal defense.
- Right to a hearing.
- Right to legal assistance and conunsel.

Confidentiality

- Right to privacy.
- Right to confidentiality.
- Right to confidentiality of information held by the tax authorities.

Transparency Access to Information

- Right to be informed about the fulfillment of tax obligations.
- Right to complete, accurate, clear and timely information.
- Right to access one's administrative file.
- Right to know the identity of the tax.

Source: Classification of taxpayers' rights and guarantees

Taking as a starting point what has been stated in this section, various relevant regulatory aspects related to the confidentiality and protection of information held by the tax authorities, transparency, as well as access and appropriate use of information in order to provide sufficient elements to promote the ethical use of information while safeguarding the fundamental guarantees of the taxpayer will be analyzed in greater detail. Thus, ensuring an appropriate balance between tax transparency and the protection of individual rights.

3.3. Confidentiality of Information and Data Protection

As mentioned above, one of the fundamental rights of taxpayers is the right to privacy and confidentiality of information held by the tax authorities. The confidentiality of tax information is a fundamental pillar in the relationship between taxpayers and tax administrations. The protection of citizens' financial, tax and personal data is essential to foster trust in the tax system and ensure respect for individual rights. The protection of information not only implies preventing its unauthorized disclosure, but also ensuring its proper use and safeguarding it against any vulnerabilities that may compromise its security. In this sense, regulatory frameworks play a crucial role in preserving the confidentiality of tax data, thereby promoting integrity and equity in financial management.

Based on the above, it is determined that the regulatory framework of each jurisdiction requires provisions focused on the protection of information in general – and in particular, of confidentiality – that are sufficiently precise, clear and detailed and expressly delimit the circumstances under which this information may be disclosed and used.

In the tax context, the preservation of confidentiality of information or tax secrecy as it is commonly known constitutes "an instrument of protection for the taxpayer, consisting of the obligation of reserve by the tax authorities in all matters relating to tax information such as tax returns and data provided by the taxpayer himself or by third parties, as well as those obtained by the authority in the exercise of its verification powers[15]. This implies that "this right of the taxpayer is correlative to the obligation of the tax authority not to disclose such information[16]."

There are several basic principles that govern the protection of the confidentiality of information; these principles are the ones that give shape and consistency to the laws and regulations that must be incorporated into the legal framework.

In this regard, the Organization of American States published a list of updated principles[17] on privacy and personal data protection that comprehensively covers all the aspects that jurisdictions should consider when designing rules, processes and procedures. These principles are:

a) **Legitimate purposes and lawfulness:** Personal data should be collected only for legitimate purposes and by lawful and legitimate means.

b) **Transparency and consent:** The specific purpose justifying its collection must be indicated along with the legal basis supporting it, the subjects to whom it will be disclosed and the rights of its owner.

c) **Relevance and necessity:** Only data that is adequate, relevant and limited to the minimum necessary for the specific purposes of its collection and further processing will be collected.

[15] Prodecon. Transparency, Tax Secrecy and Improper Use of Vouchers, 2014, p. 2. Document available at https://portal.prodecon.gob.mx/Documentos/analisis-sistemicos/estudios-tecnicos/secreto-fiscal/mobile/index.html#p=1

[16] Idem.

[17] OAS, *Updated Privacy and Personal Data Protection Principles,* 2021. Full text available at https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf

d) **Limited treatment and conservation:** The data must be processed and retained in a legitimate manner compatible with the purpose for which it was collected; its preservation must not exceed the time necessary to fulfill such purpose.

e) **Confidentiality:** The data must not be disclosed, made available to third parties or used for purposes other than those for which they were collected, except by legal mandate or with the express consent of the owner.

f) **Data security:** The confidentiality, integrity and availability of data should be protected by reasonable and appropriate technical, administrative or organizational security safeguards against unauthorized or unlawful processing.

g) **Data accuracy:** Data must be kept accurate, complete, and updated to the extent necessary for the purposes of its processing, in such a way that its veracity is not altered.

h) **Access, rectification, erasure, objection and portability:** Jurisdictions must have reasonable, agile, simple and effective methods and mechanisms to allow those persons whose personal data has been collected to request access, rectification and erasure of such data, as well as the right to object to its processing and, where applicable, the right to the portability of such personal data.

i) **Sensitive personal data:** The categories of such data and the scope of their protection should be clearly indicated in domestic legislation and regulations.

j) **Accountability:** Appropriate and effective technical and organizational measures must be adopted and implemented to ensure compliance with data protection regulations. These measures should be audited and updated on a regular basis.

k) **Transborder data flow and accountability:** (applicable only in the context of OAS members) referring to the creation of mechanisms and procedures to ensure that data controllers and processors operating in more than one jurisdiction are effectively held accountable for complying with these Principles.

l) **Exceptions:** Any exceptions should be expressly and specifically provided for in national legislation, be made known to citizens, and be limited to specific cases (national security, public order, public interest, among others).

m) **Data protection authorities:** Establish independent oversight bodies, endowed with sufficient resources, in accordance with the constitutional, organizational and administrative structure of each State, to monitor and promote data protection.

These principles must necessarily be present in the regulations of the jurisdictions in order to consider that they have a legal framework that effectively guarantees the preservation of the confidentiality of the information and the protection of the data in their possession.

Finally, with regard to the body of law in which they should be incorporated into current regulations, the OECD has pointed out that confidentiality protection rules can be found in "legislative statutes, secondary or executive regulations, or administrative guidance. Whichever the legislative instrument used, the rules should be legally binding and enforceable"[18]. Based on the foregoing, it is valid to conclude that jurisdictions may include provisions relating to confidentiality of information within the legal framework they consider most appropriate or convenient as long as it is legally valid and capable of being applied and producing full legal effects. In the same vein, there are no limitations as to the approach such legislation may take, i.e., confidentiality protection 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."[19].

3.4. Access to Public Information and Transparency

According to UNESCO, access to information can be defined as the "right to seek, receive and disseminate information held by public bodies[20]." It is one of the fundamental rights recognized by the Universal Declaration of Human Rights, as an integral part of the right to freedom of expression. As such, access to information is therefore a prerogative that has its origin in the right to information.

Transparency, for its part, could be defined as the "set of government decisions and actions aimed at providing citizens with clear, accurate, accessible and abundant information on various aspects of government performance."

However, with the evolution of open data policies, the concept of transparency has also been modified, so that it is now feasible to speak of *two levels or generations of transparency*. That is, the conventional notion of transparency (identified as first generation) is the one regulated through the laws of access to government information, its objective is broad and abstract since it seeks the promotion of the right to information in general, while the second generation, called *focused transparency*, consists of the "disclosure, by public or private entities, of public information aimed at a specific audience" [21]; that is, the authorities additionally make available to specific subjects, specific or specialized data and information.

[18] OECD, *Confidentiality and Information Security Management ToolkitConfidentiality and Information Security Management Toolkit*, OECD Publishing, 2021. page 11.

[19] Ídem.

[20] https://www.unesco.org/en/access-information-laws

[21] Organization of American States, *Access to Public Information, a Right to exercise other Rights.* 2013, pp. 17–18.

Together, the right of access to information and transparency are essential to promote democracy because they guarantee that citizens will have sufficient information to participate fully in matters of public interest. This interaction promotes accountability and forces public servants to act responsibly, resulting in greater trust in public institutions and government in general.

Open data policies and governance have become a trend that seeks to transform public management by promoting transparency and citizen participation. The concept revolves around the notion that information generated by public institutions should be available to anyone, in accessible, open and free formats that facilitate its use and interpretation.

This topic will be discussed in greater detail in the section on Data Governance in Tax Administrations.

3.5. Sanctioning Framework

One of the most important powers of the State is its penal action, defined as "the legal possibility of imposing sanctions on individuals and even on officials who infringe its provisions, or on its employees who, in the exercise of their functions, transgress its mandates or disregard its prohibitions"[22].

From the foregoing, it is clear that the State, embodied in the administrative authorities, has the power to apply sanctions to those who violate the law. The subjects susceptible of being sanctioned range from private individuals to public officials and employees who fail to comply with the rules or commit unlawful conduct.

In the context of this document, the existence of administrative sanctioning procedures contributes to ensure transparency and the protection of the rights of individuals by reducing the risk of applying disproportionate measures, avoiding arbitrariness in the exercise of state power, while preserving order and legality.

Hence, the administrative sanctioning procedure will guarantee transparency and access to information as long as it is supported by a clearly defined legal framework that ensures that the actions of the administrative authorities are subject to specific legal provisions.

In this regard, there must be a balance between access to information and the protection of taxpayers' rights; therefore, it is crucial to ensure that the disclosure of and public access to information held by the authorities is carried out in a manner compatible with the protection of taxpayers' rights and the confidentiality of sensitive information.

[22] Ossa Arbeláez, Jaime, *Administrative Sanctioning Law. Towards a general theory and an approach for its autonomy.,* Colombia, Legis, 2000, p. 126 – cited in: *Estudios en Homenaje a Héctor Fix Zamudio – El reconocimiento del Derecho Administrativo Sancionador en la Jurisprudencia Constitucional Mexicana,* Góngora Pimentel, Genaro David, IIJ – UNAM, p. 257.

Accordingly, jurisdictions should have adequate mechanisms and protocols in place to protect the confidentiality of information and taxpayer rights while granting access to public information without identifying individual taxpayers, except where expressly required by law.

This section will address the most relevant principles and aspects that should be taken into consideration when reviewing or, if applicable, designing the regulatory provisions that constitute the sanctioning framework for confidentiality, transparency and access to information.

A robust legal system must necessarily have rules and procedures aimed at ensuring compliance with legal obligations and provisions. The purpose of sanctions is to punish infringing conduct and to ensure that the offending parties do not incur in non-compliance again. In other words, they are dissuasive and repressive measures aimed at preventing repeat offenses.

In this regard, there are different types of sanctions that may be imposed under specific circumstances that may be individualized according to the nature of the infringing conduct, its seriousness, the quality of the offender and the repetition or recidivism of the conduct.

Special Law against IT and Related Crimes. El Salvador.

The criminal legislation of El Salvador in force since 1998, marginally made reference to crimes committed through the use of information and communication technologies; it was not until 2016 that the Special Law against IT and Related Crimes was enacted, establishing the specific legal treatment to be given to undue or illicit conducts carried out through the use of Information and Communication Technologies.

In this respect, it is noteworthy that this Law considers as aggravating circumstances those crimes that involve public computer programs or systems or computer systems used for the provision of health services, communications, energy supply and transport, transportation or other public services, or used for the provision of financial services, or if the offenses covered by the legislation are committed by officials, public and municipal employees, public authority or agents of authority, in which case they will be punished with the corresponding maximum penalty, increased by up to one third of the established maximum penalty and disqualification from the exercise of their profession for the duration of the sentence.

This case is a remarkable example of the interaction between administrative and criminal provisions in order to establish a comprehensive and robust legal framework focused on the confidentiality of information, ensuring its proper use and preventing its improper disclosure.

In the context of this guide, it is required that tax administrations have the power to apply effective sanctions in cases of improper use or disclosure of information, breaches of confidentiality, failure to comply with transparency obligations, etc.

In view of the above, the sanctions, according to their nature, are divided into:

a) **Disciplinary or administrative:** For example, reprimand, suspension, dismissal or disqualification of public servants in violation.

b) **Patrimonial or pecuniary:** These refer to obligations to pay amounts of money for the commission of an infraction, such as fines.

c) **Criminal:** These are applied when the infraction committed constitutes a crime and may result in deprivation of liberty or of the rights of the offender.

Now, in general, infractions and penalties related to violations of confidentiality, improper use or disclosure of information or even breaches of transparency obligations must be aligned with various principles, such as the principle of legality, proportionality, non-retroactivity and statute of limitations.

a) **Principle of legality.** It implies that the generic description of the offenses must necessarily be contained in a legal instrument. This means that, although *"sanctions may be contained in tax, public administration or criminal legislation, or in a combination of all of them (..), what matters is that due consideration is given to administrative, civil and/or criminal fines or sanctions, covering a wide range of violations of confidentiality or misuse of information*[23]*"* of transparency and access to information. This means that regardless of the legal instrument that contains them or the nature attributed to them, what is essential is that such infractions, fines and/or sanctions are formulated in a clear and precise manner and are sufficiently strong to deter any infraction or violation of the regulations.

   The principle of legality also refers to the administrative or judicial instrument in which the application of the sanction to the offender is resolved or determined in order to provide legal certainty and security to the parties involved.

b) **Principle of proportionality**. It must also be applied at two levels, initially when identifying the offense and attributing a sanction, where the legislator must maintain a balance between the offense and the corresponding sanction.

   The second level must be observed at the time the sanction is imposed, where its scope must be determined according to the specific circumstances of the case (seriousness, recidivism, damage caused by the violation, etc.).

[23] OECD, *Confidentiality and Information Security Management Toolkit*, OECD Publishing, 2021. p. 95.

c) **Principle of non-retroactivity.** This principle safeguards the guarantees of legality and legal certainty, since only the regulations in force at the time of the occurrence of the facts may be applied to determine whether they actually constitute an offense. Consequently, only the sanctions expressly contemplated in the regulations in force at the time of their occurrence may be applied.

d) **Principle of Statute of Limitations.** This refers to the fact that, in general, the passage of time will lead to the extinction of administrative offenses and penalties. However, it should be clarified that limitation period is suspended once the administrative sanctioning process is initiated.

In the case of infractions related to issues of confidentiality and security of information, improper use and disclosure of information and breaches of transparency, several factors must be taken into consideration, such as the status of the parties committing the breach (public servants – including permanent, temporary or temporary workers, or even retired workers, external workers) and the seriousness of the infraction (based on an assessment of the damage caused by the breach), among others.

This is so, since the assessment of the seriousness of an offense related to confidentiality and information security issues or to the improper use and disclosure of information must consider not only the nature and sensitivity of the information compromised, but also the context and circumstances under which the offense was committed.

Example of the classification of the seriousness of infractions. Costa Rica

An example of the distinction of the seriousness of the infractions is found in the Law for the Protection of Individuals with regard to the Processing of their Personal Data – Law No. 8968 published on September 5, 2011.

This regulation, in its articles 29, 30 and 31, classifies offenses as minor, serious and very serious, clearly describing the specific cases that fall into each category and establishing specific penalties for each case.

Minor Offenses: Collecting personal data without providing sufficient information to the data subject; collecting, storing and transmitting personal data of third parties through insecure means or mechanisms that do not guarantee the security and integrity of the data.

In this case, the applicable sanction is a fine of up to five base salaries.

Serious Offenses: Among others, collecting, storing, transmitting or otherwise using personal data without the informed and express consent of the owner; using personal data for a purpose other than *that authorized by the owner; unjustifiably refusing to grant access to a data subject to data contained in files and databases or refusing to modify, correct or delete such data upon request by the owner.*

The sanction established is a fine ranging from five to twenty base salaries.

Very Serious Offenses: Collecting, storing, transmitting or in any other way using sensitive data; obtaining personal data of a person by means of deceit, violence or threat, disclosing information whose secrecy is required by law or transferring personal information of Costa Ricans or foreigners residing in the country to databases in third countries without the consent of the owners, among others.Applicable sanctions include a fine ranging from fifteen to thirty base salaries and a suspension of up to six months.

This means that those violations involving data classified as highly confidential or critical will require a more vigorous and effective sanction than those breaches affecting less sensitive information. In this regard, the OECD has pointed out that even though "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 personal gain by one or more persons (for example due to corruption) (...) any breach of confidentiality must be taken seriously and acted upon immediately (and) appropriate actions to be taken will depend on the circumstances of the breach."[24]

In addition to the above, it is essential to take into account the protocols and regulations that jurisdictions have established on data protection and transparency, ensuring that sanctions are proportional to the magnitude of the offense in order to promote a culture of accountability and compliance in all government agencies and organizations involved.

Therefore, it is crucial for jurisdictions to establish effective monitoring and supervision mechanisms to prevent future offenses and ensure integrity and trust in information management systems. This implies that, in addition to the appropriate regulatory framework, consideration should be given to the implementation of adequate controls, ongoing staff training and a rapid and forceful response to any violation detected, in order to safeguard taxpayers' rights. This particular topic will be addressed in the chapter on the Information Security Management (ISM) framework.

The most relevant aspects to consider when implementing the sanctioning framework are as follows:

a) Identification of the subjects that the legislation will consider as obligated subjects who will be held liable for violations of confidentiality, transparency and access to information obligations.

[24] Idem.

b) Detailed description of the conducts that will be considered offenses, infractions and crimes regarding confidentiality, data protection and transparency. These conducts must be expressly defined in the legislation; the application of analogies must not be allowed in order to provide security and legal certainty to the obligated parties.

c) The types of violations may be classified according to their seriousness or the degree of damage caused by their commission.

d) Identification of circumstances that will be considered aggravating or mitigating the conduct. These conditions will be taken into account when imposing the sanction and may refer to issues such as recidivism, the intentional nature of the offense, the type of information that was violated, among others.

e) Clearly establish the procedure for imposing sanctions, indicating precisely the stages of the procedure and the manner in which each phase will be carried out.

From the above, it can be concluded that regardless of the differences in the approaches and treatment that each country decides to apply, what is crucial is to have a regulatory framework that has the required elements to protect the fundamental rights of taxpayers in this area, where each jurisdiction has established specific provisions to address the various offenses that can be committed, ranging from unauthorized access to confidential information to inappropriate disclosure of sensitive data. Penalties include fines, temporary suspension of functions or disqualification of public servants or even criminal prosecution, thus ensuring a proportional and effective response to violations of the provisions on transparency, data protection and confidentiality of information.

Country	Sanction Type	Examples of Violations	Sanction
Costa Rica	Administrative	• Non-delivery of public information. • Violation of the Law on the Protection of the Person with regard to the Processing of their Personal Data.	• Fines • Warnings or admonitions
	Criminal	• Disclosure of confidential data without authorization.	• Imprisonment • Fines
	Pecuniary	• Misuse of personal information.	• Compensation for damages
El Salvador	Administrative	• Refusal to provide public information.	• Fines • Suspension of duties
	Criminal	• Concealment of public information.	• Imprisonment • Fines
	Pecuniary	• Misuse of public funds.	• Damage Compensation or Reimbursement
Guatemala	Administrative	• Non-compliance with access to information requests.	• Fines • Disqualification
	Criminal	• Disclosure of confidential information.	• Imprisonment Fines
	Pecuniary	• Misuse of public funds.	• Compensation
Honduras	Administrative	• Failure to provide requested information.	• Fines • Warnings
	Criminal	• Unauthorized disclosure of data.	• Imprisonment Fines
	Pecuniary	• Damage to public image.	• Compensation
Panama	Administrative	• Refusal to hand over public information	• Fines • Administrative sanctions
	Criminal	• Obstruction of access to public information	• Imprisonment Fines
	Pecuniary	• Misuse of public information	• Compensation
Dominican Republic	Administrative	• Failure to provide public information	• Fines • Suspension
	Criminal	• Improper disclosure of information	• Imprisonment • Fines
	Pecuniary	• Misuse of public funds	• Compensation

International Scope

In general, the provisions contained in international tax instruments, such as the Convention on Mutual Administrative Assistance in Tax Matters, the Model Tax Convention, as well as the conventions and agreements based on such models, establish different guidelines that apply with respect to the **confidentiality and protection of information**.

Among the most relevant aspects foreseen in such instruments the following stand out:

a) Information received by the authorities of a jurisdiction – through the exchange of information – shall be treated as a secret applying the same rules and criteria as would apply to information obtained under the national laws of that jurisdiction.

b) The information may only be used for specific objectives and purposes and must always relate to the taxes that are the subject of the instrument in question.

c) The information may only be disclosed to specific persons or authorities, including courts and administrative bodies responsible for the assessment, collection, enforcement, judicial proceedings and determination of remedies.

Jurisdictions must ensure that they will preserve the confidentiality of the information exchanged under the same terms applicable to information obtained under their domestic legislation.

This implies that jurisdictions are obliged to preserve the secrecy or confidentiality of information exchanged through international instruments using the **same criteria** applicable to information collected under their national legislation. It is therefore crucial that jurisdictions have adequate domestic regulations to identify improper or unlawful conduct and sanction it appropriately in order to deter it and, consequently, protect the confidentiality and proper use of the information.

An example of this can be found in the *Standard for Automatic Exchange of Financial Account Information in Tax Matters*[25], which states, in the Comments to the Model Agreement between Competent Authorities, specifically in relation to the application of penalties and sanctions, as follows:

[25] OECD*, Standard for the Automatic Exchange of Information Financial Accounts,* OECD Publishing, 2017, page 95.

Confidentiality provisions contained in Model Agreements and other International Instruments.

Convention on Mutual Administrative Assistance in Tax Matters

Article 22. Secrecy

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 underits 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. If a Party has made a reservation provided for in sub-paragraph a. of paragraph 1 of Article 30, any other Party obtaining information from that Party shall not use it for the purpose of a tax in a category subject to the reservation. Similarly, the Party making such a reservation shall not use information obtained under this Convention for the purpose of a tax in a category subject to the reservation.

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.

OECD Model Tax Convention on Income and on Capital
Article 26 – second paragraph

2. 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.*

Model UN – Tax Convention on Income and on Capital
Article 26 – second paragraph

2. 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.

3.1. Penalties and Sanctions
35. Domestic law must impose penalties or sanctions for improper disclosure or use of taxpayer information, and tax administrations must in fact impose these penalties and sanctions against personnel who violate security policies and procedures to deter others from engaging in similar violations. To ensure implementation, such laws must be reinforced by adequate administrative resources and procedures. Tax administrations should implement a formal sanctions process for personnel and third-party providers who fail to comply with established information security policies and procedures. Policies should consider both civil and criminal sanctions for unauthorised inspection or disclosure.

Based on what has been pointed out in this chapter, it can be concluded that an adequate legal framework must guarantee a comprehensive protection of the taxpayer's fundamental rights both domestically and internationally. It is important to find an appropriate balance between access to information and transparency with respect to the protection of confidentiality and data integrity. Therefore, laws and policies related to confidentiality should be clearly established and adequately monitored to avoid abuses and ensure that the principles of transparency and access to information are respected to the extent possible.

It is essential to establish effective accountability mechanisms to ensure that confidential information is handled responsibly and used only as expressly provided for by law. This may involve the implementation of internal safeguards, such as restricted access protocols and monitoring systems, as well as external accountability through independent audits and review by regulatory and oversight bodies. These issues will be addressed in more detail in the following chapters.

4. Information Security and Protection Management

The digitization of the economy and, consequently, of tax operations has transformed the horizon of technological security for tax administrations globally. This has resulted in new challenges and requirements in terms of data protection, secure infrastructure and regulatory compliance. To meet these challenges, it is crucial for tax authorities to adopt effective cybersecurity measures and be prepared to adapt to a constantly evolving digital environment.

Thus, the efficient management of tax information protection has become an essential aspect for administrations; the gradual and continuous transition towards the digitalization of tax processes and procedures generates, consequently, a massive amount of sensitive data that requires solid protection against security threats.

In this context, the implementation of an adequate ISM framework is essential to safeguard the integrity, confidentiality and availability of tax information. Therefore, the implementation of an effective ISM framework should involve all levels of the organization in the protection of tax information, strengthening the overall cybersecurity of the administration while reducing the risk of security incidents caused by human error or negligence.

In view of the above, it is considered that the implementation of an ISM framework provides tax administrations with the necessary tools and processes to protect the integrity, confidentiality and availability of tax information, thus ensuring taxpayers' trust and strengthening compliance with their tax obligations.

This section will address the strategic points that tax administrations should take into consideration when implementing an ISM framework that effectively establishes controls and procedures to protect tax information against cyber threats and risks such as unauthorized access, data manipulation and information theft. This includes implementing access controls, data encryption, security event monitoring and password management policies, among others.

4.1. Information Security

Information security can be defined as “the process of maintaining the confidentiality, integrity and availability of an organization’s data in a manner consistent with its own risk strategy[26].” This process is accomplished through the implementation of protective measures, known as safeguards, designed to meet the security requirements of a computer system, limiting its access and handling of information. In addition to protecting the confidentiality, integrity and availability of information, it is also important to implement measures focused on preserving the authenticity, reliability, traceability and non-repudiation of information[27].

The main objectives of the security of information held by the tax authorities, for the purposes of this guide, can be concentrated in three main areas:

a) To preserve the **privacy** of the taxpayer’s data, restricting its access and disclosure.

b) To protect the **integrity** of the information by preventing its modification or undue destruction.

c) To maintain the **availability** and, if necessary, ensure the recovery of the information in due time and form.

The field of information security also includes **cybersecurity**, which is a branch specializing in the protection of computer systems and networks against unauthorized access, malicious activities and damage, i.e. it focuses specifically on the protection of technologies designed to facilitate access to and handling of information.

Although both branches have the protection of confidential information as a common objective, the main difference between them is that while cybersecurity protects devices, systems and technologies connected to the Internet, information security also extends its protection to any offline information (i.e. data, physical and digital records, intellectual property, among others).

Considering the above, tax authorities need to design and implement strict comprehensive security protocols, i.e., covering both technological systems and operational and administrative aspects in order to deter, stop and prevent unauthorized access, data manipulation or loss of sensitive information. This includes the adoption of advanced encryption measures, intrusion detection systems and ongoing staff training in secure data management practices.

[26] As defined by the *National Institute of Standards and Technology.* https://www.nccoe.nist.gov/data-security

[27] This attribute allows testing the participation of parties in a communication, that is, gives certainty that a party cannot later originated data.

In view of the above, it can be noted that the ISM framework focuses on securing all information assets of the tax administration, including confidential data, tax information, financial information, etc. The primary objective of this framework is to ensure the confidentiality, integrity and availability of information throughout its life cycle, from creation to disposal.

The following are some of the relevant issues that tax authorities should take into consideration when designing and implementing their information security strategies.

4.2. International Standards on Information Security

International information security standards are sets of best practices, guidelines and technical requirements designed to promote the security and protection of information in organizations and systems globally. The primary objective of these standards is to support the establishment and implementation of sound information security practices, protect sensitive data, manage risks and comply with applicable regulations in different jurisdictions worldwide.

In relation to the above, the International Organization for Standardization (ISO)[28] is an international non-governmental organization created in 1947 that comprises different technical committees made up of groups of experts in various fields whose objective is to design international standardized norms. It currently has 171 member countries whose experts have developed more than 20,000 international standards and related documents.

One of the most important standards designed by ISO is the **ISO/IEC-27000**[29] series focused on information security management. This standard encompasses more than a dozen more specific standards focused on information security management and ISM systems. Together, these standards provide a comprehensive framework for establishing, implementing, maintaining and improving information security within the organization.

The ISO/IEC-27000 series was initially developed in 2016, in 2018 it was replaced by the standard currently in force and is expected to be replaced by the ISO/IEC WD – 27000 series in the coming years.

[28] https://www.iso.org/es/home

[29] This series was developed by a Joint Technical Committee formed by experts of the International Organization of Standards and the International Electrotechnical Commission (IEC), which is why it is identified as ISO/IEC 27000 series.

The ISO 27000 standard consists of several standards, the best known and most widely used being:

a) **ISO-27001.** This is the main standard in the series and establishes the fundamental requirements for the proper implementation of an ISM system. This standard establishes the operational, technological and even normative-regulatory framework required for the systematic and consistent implementation of information security measures.

b) **ISO-27002 Standard**. It establishes guidelines and recommendations regarding the implementation of security controls, access to information and maintenance of technological systems.

c) **ISO-27005 Standard**. Encompasses the main guidelines on security risk management (identification, evaluation and treatment).

d) **Complementary standards**. (i.e. ISO-27003, ISO-27004, ISO-27006) focused on issues related to applicable measurements and metrics, ISM systems certification, among other issues.

It is necessary to clarify that there is no single ISM standard, so tax administrations may apply the one they consider most appropriate or according to their needs and circumstances[30]; however, taking into consideration that the ISO/IEC-27000 series is internationally recognized as the standard that encompasses the most commonly applied standards and best practices in information security, it will be taken as a reference in this work.

However, regardless of the standard that tax administrations use as a basis for the implementation of the ISM framework, such adoption will bring multiple advantages for the tax authority, such as:

a) The tax authority will be able to react in an agile manner to address security incidents and events by implementing physical, administrative and technological controls specifically designed to manage aspects such as access (both internal and external personnel), hardware, software, operations and communications.

b) Information security protection will cover all types of information held by the tax authority: printed or written on paper, stored electronically, transmitted by electronic means and even verbally.

c) The authority will be able to adequately assess the risks to which it is potentially exposed based on a procedure and will have sufficient elements to create the optimal plan for its attention and treatment.

[30] Among the standards on information security, there is also *NIST Cybersecurity Framework* developed by the *National Institute of Standards and Technology of the United States* or the standards developed by the European Union known as the *General Data Protection Regulation* or GDPR.

d) The tax administration will establish, in parallel, the mechanisms for legal and regulatory compliance related to the adequate use and handling of the information held by the tax authority.

e) As a consequence of the implementation of the ISM framework, the confidence of taxpayers, other government agencies, other tax authorities and society in general will increase.

The above corroborates the benefits of tax administrations establishing processes and mechanisms aimed at protecting information by preserving its confidentiality, integrity and availability.

4.3. Implementation of the ISO/IEC-27000 Series

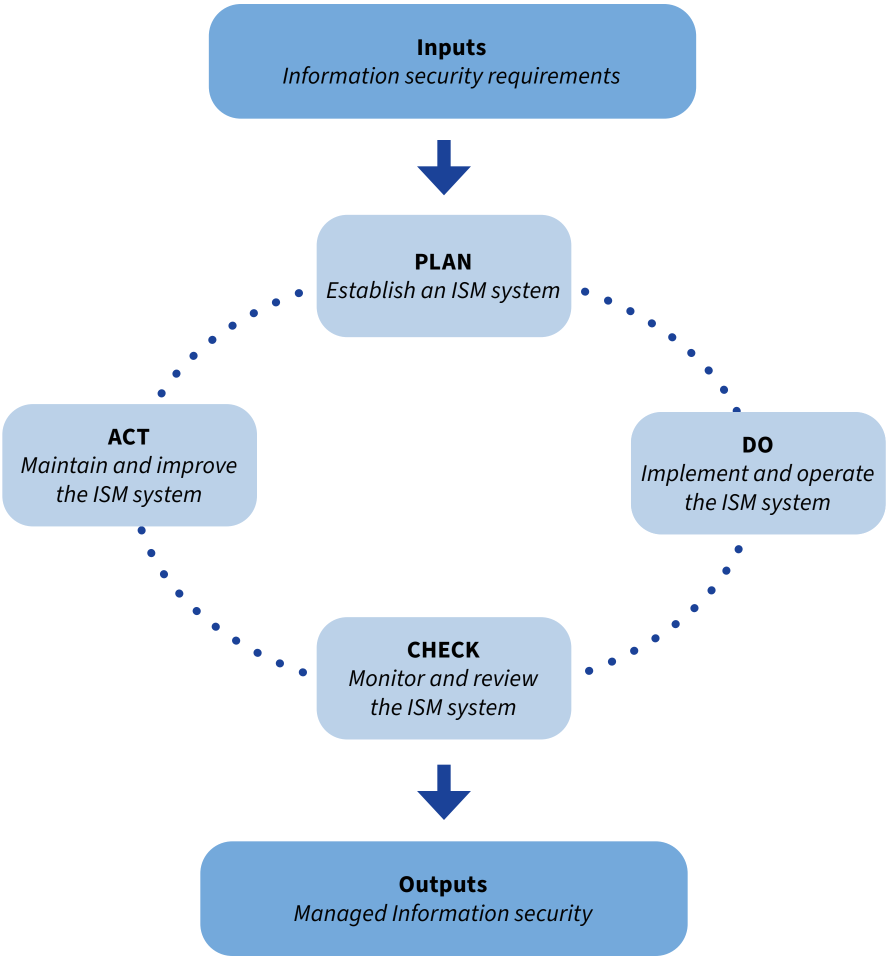
The 27000 series is based on the Deming Cycle, which was designed as a method of continuous process improvement that is implemented in different stages or phases. The Deming Cycle is also commonly referred to as the PDCA (Plan, Do, Check, Act) Cycle.

In the context of tax administrations, the ISO/IEC-27000 series can be adapted by implementing specific access controls for tax management systems, network monitoring and periodic audits to ensure the protection of taxpayer data.

Generally speaking, it can be noted that the PDCA Cycle, applied to the context of information security, involves "developing and implementing an information security framework and plan, implementing the security control mechanisms as planned, verifying that the plan is working properly, and continuously improving the plan and controls, reinforcing those activities that are working properly and modifying those that are not[31]."

In relation to the above, the Global Forum has schematized the cycle in the following way:

[31] OECD, Confidentiality and Information Security Management Toolkit, Op Cit., page 14.


Inputs
Information security requirements
PLAN
Establish an ISM system
DO
Implement and operate the ISM system
CHECK
Monitor and review the ISM system
ACT
Maintain and improve the ISM system
Outputs
Managed Information security

Source: The PDCA cycle in Information Security Management

As seen, the PDCA Cycle is an essential methodology for managing data safety in the hands of the tax administrations. Its cyclical focus allows tax administrations to continuously implement and optimize their security practices. Also, the adoption of the PDCA Cycle guarantees that the tax administration will have effective security measures but that in the long term, it may easily adapt to new threats and risks which may arise on security issues.

In general terms, the PCDA Cycle is explained as follows:

a) The first phase corresponds to the **PLAN** phase, through which the tax administrations must identify and evaluate the potential risks to which the security of the information held by the authority is exposed. This analysis also includes the review of the applicable regulations, the evaluation of possible vulnerabilities of the systems so that, subsequently, policies and procedures are established to ensure compliance with regulations and the protection of tax data and information.

b) In the second stage, identified as the **DO** phase, the tax authority will implement the security measures established in the planning stage; that is, it will install physical and logical access controls, detection systems, and train personnel in secure practices for handling tax information. This stage is fundamental in the cycle since it allows mitigating risks and strengthening the security of the administration.

c) The **CHECK phase** focuses on monitoring and evaluating the performance of the implemented security measures. Such monitoring is carried out through the execution of internal and external audits, penetration tests, log analysis and security incident reports. The results of such evaluations allow us to identify possible areas for improvement and adjust security strategies to ensure their continued effectiveness.

d) Finally, in the **ACT** phase, the necessary corrective and preventive actions are carried out in response to the findings and recommendations derived from the previous phase. This may involve updating policies and procedures, implementing new security controls or improving staff training.

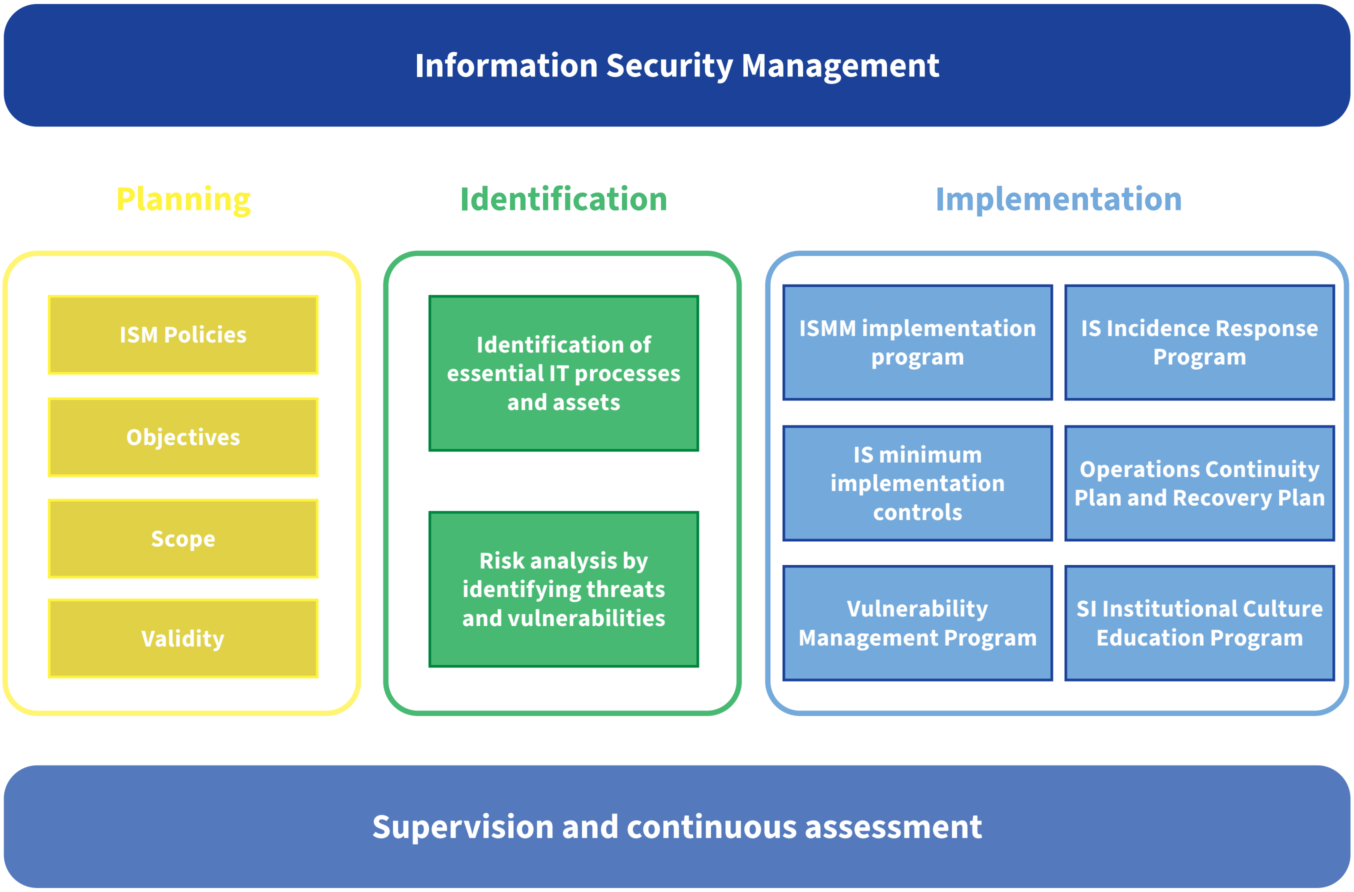
Based on the above, the OECD recommends a roadmap comprised of six fundamental steps[32] for tax authorities to carry out the implementation of the ISM framework. It should be noted that this route is designed to be implemented within the framework of the exchange of information; therefore, for the purposes of this document, it has been adapted to be applied to all tax administration activities and -if applicable- to be extended to the exchange of information, in any of its modalities.

Step 1. Scoping of the ISM Framework

The implementation of an ISM Framework for tax administrations refers to the adoption of a set of strategies, policies, procedures, controls and practices to ensure the adequate protection of tax information. This framework provides a structured and systematic guide to manage information security risks and protect data assets against internal and external threats that may arise.

This box contains the translation of the image above.

[32] OECD, Confidentiality and Information Security Management Toolkit, Op Cit., page 15.


Information Security Management
Planning
Identification
Implementation
ISM Policies
Objectives
Scope
Validity
Identification of essential IT processes and assets
Risk analysis by identifying threats and vulnerabilities
ISMM implementation program
IS Incidence Response Program
IS minimum implementation controls
Operations Continuity Plan and Recovery Plan
Vulnerability Management Program
SI Institutional Culture Education Program
Supervision and continuous assessment

Source: Example ISM Framework design

Generally, the starting point for the design of the ISM framework is the **information lifecycle**, since knowledge of the information lifecycle makes it possible to manage data from the time it is generated or *enters* the authority's sphere of competence until its destruction, once it has been used.

In this sense, the information lifecycle is divided into five phases:

a) **Data creation**: Referring to the collection of information carried out by the authority. Such information comes from various sources and may be presented in different formats. Ideally, the authority should evaluate the quality and relevance of the information to determine its usefulness in the future

b) **Data storage**: The authority shall consider how the data is structured in order to determine the type of storage that will be required. In addition, the authority will assess the infrastructure for security vulnerabilities and the data may be subjected to different types of processing (i.e. encryption and/or data transformation) as a measure to protect against eventualities and maliciousness. This also ensures that regulatory requirements regarding confidentiality and privacy of information are met.

c) **Use of information**: The information shall be made available to authorized subjects. The tax administration must establish rules and regulations to define the specific parameters under which the information may be accessed. This aspect is essential, as it must clearly specify the circumstances under which access may be granted to other authorities (including foreign authorities, in the case of exchange of information) and the public in general. From the operational and technological point of view, policies and procedures should be developed to ensure the accessibility and availability of clean and useful data, allowing its efficient and secure handling.

d) **Archiving of information**: Tax administrations shall ensure that once data has been used it shall be archived appropriately, allowing access and restoration if required (e.g. in case of litigation or criminal investigations). The tax authorities, in parallel, should establish guidelines that clearly define the timeframes and terms under which the information will be archived.

e) **Disposal of information**: Refers to the secure destruction of information once the retention periods indicated in the preceding paragraph have elapsed.

Step 2. Setting ISM policies

Tax authorities should set out in an ISM policy document the guidelines for the overall security framework. In general, the ISM framework should have clearly defined **objectives**[33], a comprehensive policy that defines the scope of the ISM system and overall objectives and reflects the authority's commitment to achieving them.

A policy is considered *comprehensive* when it covers the following general areas of security: human resources, access management, information technology security, information protection and operations management.

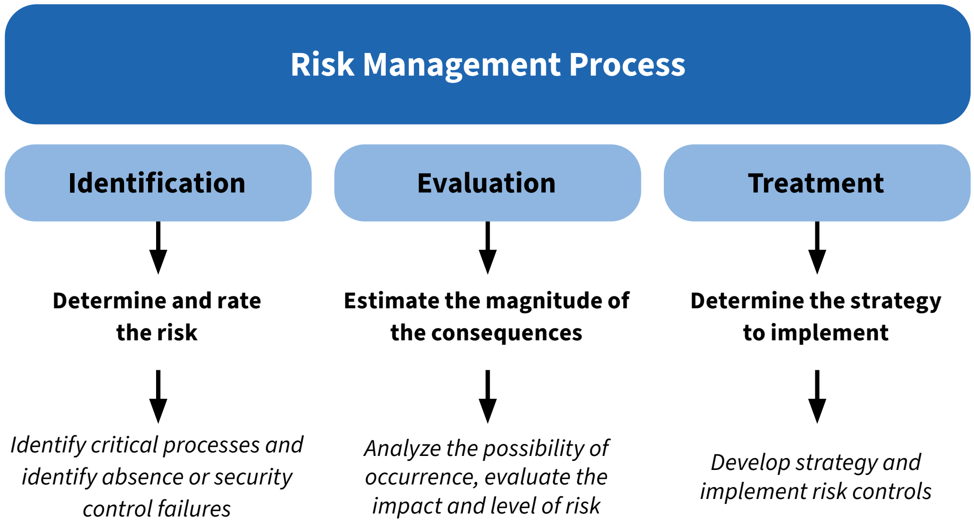
Furthermore, the ISM framework should set forth the criteria for information technology security, physical security, human resources security and business continuity, as well as clearly delimit the roles and responsibilities of the personnel in charge of information security.

In connection with the above, the tax authority must implement adequate operational measures integrated with business operations. Ideally, these measures will be set forth in a manual or similar document compiling the policies, processes, procedures and controls designed to mitigate and/or eliminate potential information security risks.

[33] For example, protect sensitive information in accordance with confidentiality and information security standards, mitigate risks through security controls, etc.

Step 3. Identifying and Managing Security Risks

It is mandatory that tax administrations systematically manage information risks to which they are exposed through a rigorous and comprehensive risk management process. A specific methodology for risk management may be developed within the ISM system or the administration's integral methodology may be adapted and aligned with ISM objectives and information security criteria.


Risk Management Process
Identification
Evaluation
Treatment
Determine and rate the risk
Estimate the magnitude of the consequences
Determine the strategy to implement
Identify critical processes and identify absence or security control failures
Analyze the possibility of occurrence, evaluate the impact and level of risk
Develop strategy and implement risk controls

In addition, periodic monitoring and reviews, risk assessment criteria (generally measured through the evaluation of the potential impact in the event that the risk is manifested), risk controls, treatment options, reporting of findings and results, etc., should be considered.

Provisions related to risk management contained in the ISM Policies. Spain.

An example of how general policies related to risk management can be incorporated is found in the Resolution of November 8, 2012, which approves the information security policy of the State Agency for Tax Administration. This document includes the general ISM policies that are later reflected in manuals, guides, and other internal documents for implementation by the tax administration staff.

Risk Management

1. Risk management must be carried out continuously on the information system and include an advanced risk analysis that evaluates residual risks and proposes appropriate treatments.

2. Risk management on the information system will be aligned with the risk management established by the Tax Agency, focused on the organization's Risk Map.

3. The Commission for Security and Control of Tax IT, in the exercise of its functions, will be responsible for analyzing and evaluating the operational risks of the services in order to establish the corresponding preventive measures.

4. For the risk assessment, the recommendations published for the field of Public Administration will be taken into account, especially the guidelines developed by the National Cryptologic Center.

Step 4. Establishing Specific Policies, Processes, and Procedures to Ensure Continuity of Operations.

Once risk analyses have been performed and appropriate controls selected for their treatment, it is imperative that the tax administration formalizes and documents these controls in its policies, processes and procedures. This systematic approach ensures that all aspects of risk management are consistently integrated into the entity's regulatory framework. The documentation should include clear descriptions of the applicable controls, as well as their objectives, responsible parties and implementation methodology, thus ensuring traceability and transparency in tax management.

Likewise, tax administrations must have measures specifically designed to manage and maintain the continuity of operations in the presence of events that alter their operation. These measures guarantee the continuous availability of services and ensure that the authority will have sufficient means to act in the event of possible interruptions caused not only by cyber-attacks or technical failures, but also by natural phenomena or even social issues.

Similar to risk assessment, the authorities must conduct an assessment to determine the conditions in which the tax administration operates in order to identify the security requirements that need to be implemented, adjusted, modified, or replaced.

Thus, the management process begins with the identification of possible scenarios that could affect or alter the operations of the tax administration. Subsequently, the potential impact of each scenario will be evaluated and documented. Based on this evaluation, a **Business Continuity Plan (BCP)** will be designed that includes testing criteria and a review of the plan, as well as the corresponding training.

The BCP must indicate the detailed processes and procedures that should be executed to ensure that the tax administration will be able to operate correctly or even recover or restore its functioning in case a contingency or disruption occurs.

Relevant Aspects of the Continuity Action Plan of the Internal Revenue Service (IRS) of the United States.

In 2020, the IRS updated the Tax Collection Manual to include new measures aimed at addressing the challenges arising from the COVID-19 pandemic.

Some of the most relevant provisions are:

- *The IRS must be able to continue performing its essential activities during any emergency for a period of up to 30 days or until normal operations can be resumed.*
- *The IRS must have the capability to be fully operational at its continuity facilities as soon as possible after the occurrence of an emergency, but no later than 12 hours after the activation of continuity operations.*
- *The IRS must safeguard its resources, facilities, and vital records, and ensure official access to them. It must also take steps to hire and/or allocate the necessary personnel and resources for continuity operations in the event of an emergency.*
- *The IRS must take steps to ensure the availability and redundancy of critical communication capabilities at continuity sites in order to support connectivity among key government leadership, IRS organizational elements, other departments and executive agencies, critical partners, and the public, as well as to identify, train, and prepare IRS personnel capable of relocating to designated facilities that are suitable during the contingency.*
- *The IRS must make arrangements for reconstitution capabilities that allow for recovery from a catastrophic emergency and the resumption of normal operations.*

An adequate BCP must, at a minimum, contain provisions related to issues such as: (i) key systems and priority operating order, (ii) essential and non-essential activities and services[34], (iii) backup copy(ies) preparation, (iv) essential personnel for the basic functioning of the administration, (v) critical information (also considering its format and method of storage and transfer, if applicable), (vi) measures for restoration (including whether it should be gradual or total, depending on the type of incident).

The last phase of the business continuity management process focuses on verifying the effectiveness of the BCP and the continuous review it must undergo. For this purpose, drills can be conducted to assess the preparedness of the tax administration against potential threats and contingencies to which it is exposed.

Paso 5. Training and Staff Development

Staff training in ISM is a fundamental pillar for the effectiveness of the policies and procedures designed to manage security risks. It is crucial that each member of the tax administration fully understands not only the current regulations but also the importance of their application. This training must be comprehensive and ongoing, adapting to updates in policies and to new threats that may arise.

Likewise, constant evaluation of the training received is essential to ensure its effectiveness; therefore, the implementation of feedback mechanisms and periodic review allows for the identification of areas for improvement and the adaptation of training content to the specific needs of the personnel and emerging trends in security. This dynamic approach not only contributes to the professional development of the team but also ensures that the tax authority is, as much as possible, at the forefront of protection against technological risks and threats, maintaining a safe and efficient environment.

Step 6. Verification of Effective Adoption of the ISM System

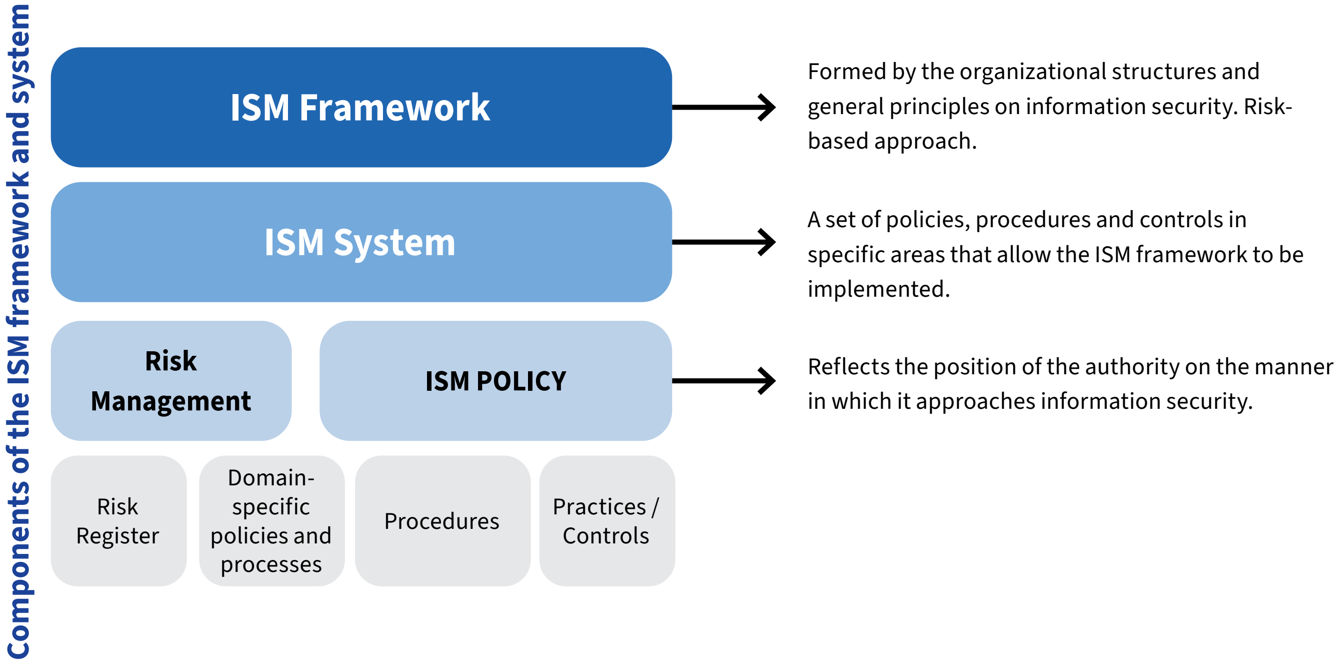
The tax administration must establish a periodic verification program that evaluates the effectiveness of the application of the ISM system by its personnel. This program should include internal audits and compliance reviews that allow identifying whether the defined policies, processes, and procedures are being implemented uniformly and aligned with the provisions of the ISM framework itself. Systematizing these

[34] The OECD, in the publication titled *Tax Administration Responses to COVID-19: Business continuity considerations*, defines essential activities as time critical functions whose failure even for hours would impact on the administration's business systems, people, buildings and suppliers resulting in an unacceptable level of disruption to its role, loss of service to its customers, or damage to its reputation. Document available at: https://read.oecd-ilibrary.org/view/?ref=133_133006-nruwv5tdpl&title=Respuesta-de-las-administraciones-tributarias-al-COVID-19-Consideraciones-acerca-de-la-continuidad-de-actividades-y-servicios

evaluations will allow for the collection of relevant data on adherence to the system, facilitating informed decision-making for continuous improvement.

In addition, mechanisms must be established to communicate the results of audits and the corrective actions derived from these evaluations, in order not only to optimize the implementation of the ISM framework but also to reinforce the institutional commitment to security and the protection of sensitive data.

Based on the previously described, the ISM Framework must be composed of the following elements.:


Components of the ISM framework and system
ISM Framework
Formed by the organizational structures and general principles on information security. Risk-based approach.
ISM System
A set of policies, procedures and controls in specific areas that allow the ISM framework to be implemented.
Risk Management
ISM POLICY
Reflects the position of the authority on the manner in which it approaches information security.
Risk Register
Domain-specific policies and processes
Procedures
Practices / Controls

The following chapter will address various aspects related to the security management of ITs in order to provide tax administrations with sufficient elements to carry out an effective implementation of the ISM framework suitable for their needs and requirements.

5. Information Technology Security Management

The information technology security management (ITSM) framework focuses on the protection of information technology systems that support and manage the critical information of the organization; that is, it protects the networks, servers, applications, and devices that process, store, and transmit data. The main objective of the ITSM framework is to ensure that these systems are protected against cyber threats and operate securely and efficiently.

As indicated in the previous chapter, the ITSM framework focuses on ensuring the confidentiality, integrity, and availability of all critical information assets of the organization, while the ITSM framework focuses on protecting the systems and technologies that support and manage that information. This means that both frameworks are complementary and must work together to ensure comprehensive protection of the organization's assets.

Now, the ITSM framework is not limited solely to the mere application of technical controls or to exclusively technological issues. The scope of the ITSM framework also extends to the organizational domains of the tax administration; that is, top management must foster and promote an organizational culture that prioritizes security through continuous staff awareness and training, the assignment of clear and well-defined roles and responsibilities, and integrates security practices and policies throughout the information lifecycle.

From the above, it follows that tax administrations that need to implement a comprehensive security system within their organization must establish a comprehensive approach that, in addition to incorporating policies and measures for information protection, implements technical and operational controls in combination with the creation of a cultural environment that fosters and prioritizes security.

What are the requirements for a Security Officer?

The Chief Security Officer (CSO) must be highly qualified and have specific experience to develop the strategy and initiatives related to security to protect the company's assets, data, and infrastructure. This person will not only develop and implement comprehensive security strategies, but must also be capable of working with interdisciplinary teams to identify risks, devise preventive measures, and ensure compliance with regulations related to infrastructure and cybersecurity.

Objectives of the person in this role

- *Develop and implement a comprehensive security framework to protect the assets and infrastructure of the tax administration.*
- *Design and implement security policies, procedures, and protocols to mitigate risks and maintain a safe environment.*
- *Investigate and oversee incident response activities, including investigations, root cause analysis, and the development of corrective actions.*
- *Collaborate with interdisciplinary teams to assess risks, identify vulnerabilities, and devise preventive measures.*
- *Establish and maintain strong relationships with external stakeholders, such as regulatory agencies, law enforcement, and industry associations.*
- *Lead security awareness programs and training initiatives to educate employees on best practices and potential threats.*

Main tasks

- *Conduct security audits and risk assessments regularly to identify vulnerabilities and ensure compliance with relevant regulations.*
- *Implement and manage security technologies, such as firewalls, intrusion detection systems, and access controls.*
- *Ensure the organization complies with applicable global security laws, regulations, and standards.*
- *Monitor security systems and networks for potential threats, investigating and mitigating security incidents in a timely manner.*

- *Oversee the management of physical security measures, including access controls, CCTV systems, and security personnel.*
- *Develop and maintain incident response plans, ensuring timely and effective responses to security breaches.*
- *Manage records, documentation, and reports to demonstrate compliance and facilitate audits.*
- *Collaborate with internal teams to integrate security considerations into the development of new products and services.*
- *Stay updated with the latest trends, technologies, and regulatory changes in security, ensuring the continuous improvement of the security function.*

Expected skills and qualifications

- *University degree in computer science, information security, or a related field. Masters in cybersecurity, information assurance, or a related field.*
- *Relevant certifications such as Certified Information Systems Security Professionals (CISSP), Certified information security manager (CISM) o Certified in Risk and Information Systems Control (CRISC).*
- *Over 7 years of experience in a senior security management role, with a proven track record in developing and implementing security strategies and frameworks.*
- *Excellent knowledge of laws, regulations, and industry standards related to infrastructure security within an organization.*
- *Deep understanding of cybersecurity, data protection regulations, and industry best practices.*
- *Strong leadership and communication skills, with the ability to effectively collaborate with interdisciplinary teams and senior management. Ability to drive cultural change and integrate a security-conscious culture within the organization.*
- *Analytical mindset and strong problem-solving skills to assess risks, analyze complex security issues, and develop appropriate solutions.*
- *Up-to-date knowledge of emerging threats, trends, and security technologies.*
- *Experience in conducting security audits, risk assessments, and incident response process management.*
- *Proficiency in the English language.*

This chapter will address the main measures and best practices related to the effective implementation of the ITSM framework in a comprehensive manner with the aim of establishing a secure infrastructure alongside a reliable organizational climate within tax administrations.

5.1. Comprehensive Management of Human Capital

The first element to consider as part of the ITSM framework implementation refers to the management of workers as well as other individuals who interact with the tax administration either through an employment contract, supply contract, or service provision.

Based on the above, it is important to distinguish between the concepts of *human resources* and *human capital* and to point out the main differences between them, as they are often used interchangeably as synonyms.

Human resources can be defined as the set of practices, processes, and administrative procedures aimed at managing human resources within an organization. This includes functions such as recruitment, performance management, compensation and benefits administration, training and development, among others.

In contrast, **human capital**, according to the OECD, is defined as "the combination of innate aptitudes and skills of individuals, as well as the qualifications and learning they acquire through education and training." [35] This notion primarily highlights the capacities, knowledge, and skills of the workers in an organization, which implies elevating the traditional notion of human resources by integrating all personnel-related functions into a cohesive strategy.

Thus, a comprehensive view of the human element as part of an institution includes both the purely personal or individual aspect and the strategic management in accordance with the objectives and approaches of the institution itself. For these purposes, then, the comprehensive management of human capital encompasses, in the first instance, the general administration of the staff working in the organization, personal development (along with the investment it entails) in conjunction with the philosophy or policies governing the specific management of administration and the contribution that the staff makes to the overall strategic management of the organization.[36]

[35] OECD, *OECD Insights. Human Capital: How what you know shapes your life. Abstract in Spanish., OECD Publishing, Paris, 2007. Page 2*. Document available at https://www.oecd-ilibrary.org/docserver/9789264029095-sum-es.pdf?expires=1721158015&id=id&accname=guest&checksum=0B33A3E116BBA88CA0AA16B137FEB6E9

[36] Rüdiger Pieper (editor), *Human Resource Management: An international comparison.*, Ed. De Gruyter, Berlin, 1990. Publication available at: Human Resource Management: An International Comparison – Google Libros

In line with the above, it is valid to point out that human capital management involves issues that go beyond the assignment of roles and responsibilities, as it considers employees as fundamental elements for achieving the organization's objectives and, therefore, it is essential to incorporate mechanisms that favor and stimulate the development of their competencies.

Thus, Human Resource Management (HRM) consists of the "design and implementation of tasks such as recruitment and selection of personnel, compensation management, performance management, and training."[37] Through this management, the parameters that the organization requires to ensure operational efficiency and safeguard the confidential information held by tax administrations will be established.

Now, in the case of tax administrations, the effective management of human capital becomes increasingly relevant in the context of the effective implementation of the ITSM framework due to the technical and highly specialized nature of the functions performed by their employees. Public officials must not only have solid knowledge of tax regulations but also in technologies, information security, and the ethical use of the information in their possession. Considering this, the selection and training of employees and the implementation of control and security measures throughout the entire lifecycle of personnel are essential elements that ensure the operational effectiveness of the tax administration.

Additionally, tax administrations must extend certain security and control measures to individuals who have a different employment or contractual relationship from that of *regular* or *permanent* employees, such as temporary employees or external contractors.

The following sections will specifically address the most appropriate rules and control measures to effectively implement the ITSM framework.

The Personnel Lifecycle

In general terms, the employee lifecycle refers to the set of stages or phases that an employee goes through from recruitment and hiring to leaving the organization. This cycle can vary in detail according to the specific policies and practices of each organization or encompass different stages of the employment relationship.

However, it can be established that the employee life cycle is generally divided into three main phases:

a) **Recruitment and Hiring**: It involves the proactive search for talent to incorporate into the organization once they demonstrate they possess the necessary knowledge and skills to fill a vacancy. As part of the

[37] OECD, Overview of Public Administrations of Latin America and the Caribbean 2020, OECD Publishing, Paris, 2020, p. 110. Document available at: https://doi.org/10.1787/1256b68d-es

process, different filters will be applied, such as interviews, assessments, background checks, among others. The phase concludes once the job offer is accepted by the candidate and is formalized with the signing of the employment contract.

b) **Training and Professional Development:** It begins with the induction phase, in which the employee will receive training in order to acquire the necessary knowledge to adequately integrate into the organization. Training is the next phase in which the employee is given technical, theoretical, and practical knowledge with the goal of optimizing their performance by improving and increasing their competencies and skills.

c) **Labor Disengagement:** It occurs when the labor relationship is voluntarily terminated by the employee, the employer, or both (for example, through resignation or retirement) or involuntarily (through dismissal, termination, etc.). This disengagement must be carried out in a structured manner through a process that includes measures aimed at safeguarding the security and confidentiality of information upon the departure of an employee.

From hiring to the termination of the employment relationship, each phase requires tax administrations to establish rigorous measures to mitigate the risks associated with potential data breaches and violations that officials may commit. By implementing robust security protocols and adhering to strict regulatory requirements, tax administrations can maintain public trust and fulfill their vital role in fiscal governance.

Implementation of Human Capital Controls

In general, human resources controls are defined as the ‘legal and administrative policies and procedures applicable to the management of human resources in the tax administration (generally, internal staff and contractors), aimed at ensuring that they respect and protect the confidentiality of tax information.”[38]

This section will briefly address the control measures that are recommended to be implemented in each phase of the work life cycle.

Controls During the Hiring Phase

Specifically, these controls refer to the checks and tests that the tax administration will carry out to ensure the confidentiality of candidates (and potential employees) regarding the handling of confidential information. Such measures include conveying to the candidate information regarding the importance of security and confidentiality of information (usually during the interview), the application of processes for checking

[38] OECD, Confidentiality and Information Security Management Toolkit, Op Cit., page 29.

criminal, financial backgrounds, and any other type of in-depth investigation that the tax administration requires to execute according to the type of position being offered.

It is important to highlight that these verifications must be updated or reapplied periodically throughout the employment relationship; in the case of external contractors and suppliers, the tax administration must also carry out these checks and verifications, adapting them to the nature of the functions, activities, or work that these contractors and suppliers will perform.

In any case, tax administrations are obligated to inform candidates, newly hired employees, contractors, and suppliers regarding the functions, obligations, responsibilities, and penalties applicable in matters of confidentiality and information security.

Controls Related to the Employment Relationship

It is recommended that the tax administration implement continuous training and awareness campaigns for workers on information security and confidentiality. *Training* refers to the acquisition and development of knowledge, skills, and competencies to incorporate confidentiality and security into tax processes, while *awareness* communicates to staff about the risks and threats related to security.[39]

Controls Regarding the Termination of the Employment Relationship

They refer to the policies and processes applicable when the employment relationship is terminated in order to protect sensitive information. The objective is to ensure that the confidentiality of the information will be maintained even after the termination of the employment relationship.

Among the most important applicable control measures are:

a) *Recovery of official assets:* The employee must return the identification, computer equipment, telephone, and any other similar device that was provided to the worker for the performance of their duties.

b) *Revocation of rights:* In order to preserve the security and confidentiality of the information, all access permissions (physical and logical) granted to the employee must be revoked. This point will be addressed in greater detail in the following section.

[39] Ibidem, page 35.

5.2. Access Control

The fundamental principle that governs access control policies specifically focused on the security and confidentiality of information is the **principle of need to know**. This principle implies that only users who have a legitimate reason[40] to access information held by tax authorities. Closely related to this is the **principle of minimum privilege**. The difference between the two lies in that the former is aimed at the individuals who will be authorized to view certain confidential information, while the latter pertains to the privileged access rights of users and their respective accounts. The adoption of these principles will necessarily require the implementation of controls over user access rights and the management of the accounts assigned to them.

In light of the above, it is necessary for the tax administration to clearly define the roles and responsibilities, as well as the types of users who will be granted the minimum rights of access to the data.

In that context, the type of users who will potentially be granted access to the information held by the tax authorities depends on the role and level of access to the information that will be granted. Accordingly, the types of users generally include end users, system administrators, and audit personnel. End users are those who interact directly with the information systems in their daily activities, while system administrators are responsible for the configuration, maintenance, and security of the technological platforms. On the other hand, audit personnel are responsible for evaluating compliance with security policies and the effectiveness of the established controls.

Design and Implementation of General Information Security Policies. Mexico.

The Tax Administration Service (SAT, in Spanish) published the document that consolidates the requirements for the proper implementation of information security policies.

General Information Security Policy.

Objective: *To ensure that all personnel of the organization and third parties act and make decisions in accordance with the organization's criteria and definitions regarding information security, in addition to ensuring the full commitment and active participation of senior management in information security.*

[40] Generally, the legitimate reason is directly linked to the role and responsibilities that the job function requires and specifies.

Design:

1. *There must be a formally documented General Information Security Policy.*
2. *It must be signed either by hand or through an electronic signature by the general management, representative, or legal proxy.*
3. *It must include a section describing the commitment and active participation of the general management regarding information security.*
4. *It should include the definition of information security, that is, how the organization conceives the concept of information security.*
5. *It should include references to regulations, current legislation, and applicable frameworks regarding information security for the organization.*
6. *It should include the organization's information security objectives.*

   (a) Must be aligned with the organization's strategy (b) Must consider the protection of personal data and taxpayer information, and (c) Must consider compliance with legal and regulatory requirements.

7. *It should include the roles and responsibilities of information security and elements such as:*

   (a) RACI responsibility assignment matrix or (b) Organizational chart with job descriptions or (c) Job profiles with detailed activities, and (d) Disciplinary measures, sanctions, and/or penalties in case of non-compliance with the policy.

8. *Must include guidelines to ensure the confidentiality, integrity, and availability of information for both internal staff and external personnel to the organization.*
9. *Must have a section for change control and versions of the policy with dates, participants, and change controls.*
10. *Must define a review period for the policy, at least every 12 months.*

Now, the control measures that tax administrations must implement to protect the integrity, confidentiality, and availability of the sensitive information they handle can be classified into two categories: physical access controls and logical access controls, both of which are explained further below.

For the purpose of designing and implementing the policies governing the allocation of physical and logical access controls, tax authorities must carry out at least one **risk and threat assessment** through which the authority thoroughly analyzes the risks and threats it faces. This includes identifying critical assets that need protection, such as facilities, data centers, servers, network equipment, systems, and applications, among other resources. The risk assessment will help the authority prioritize which security controls will be implemented and under what terms.

For these purposes, the tax administration must establish various **criteria for the assignment, modification, and revocation of access rights**. The authority must first determine whether the access rights and controls will be granted based on the roles of each user or if they will be granted at its discretion.

An approach that may prove useful when defining the criteria based on which access to information will be granted is the one presented by the CIAT in the document titled "ICT as a Strategic Tool to Enhance the Efficiency of Tax Administrations,"[41] in which the implementation of three levels of security is recommended:

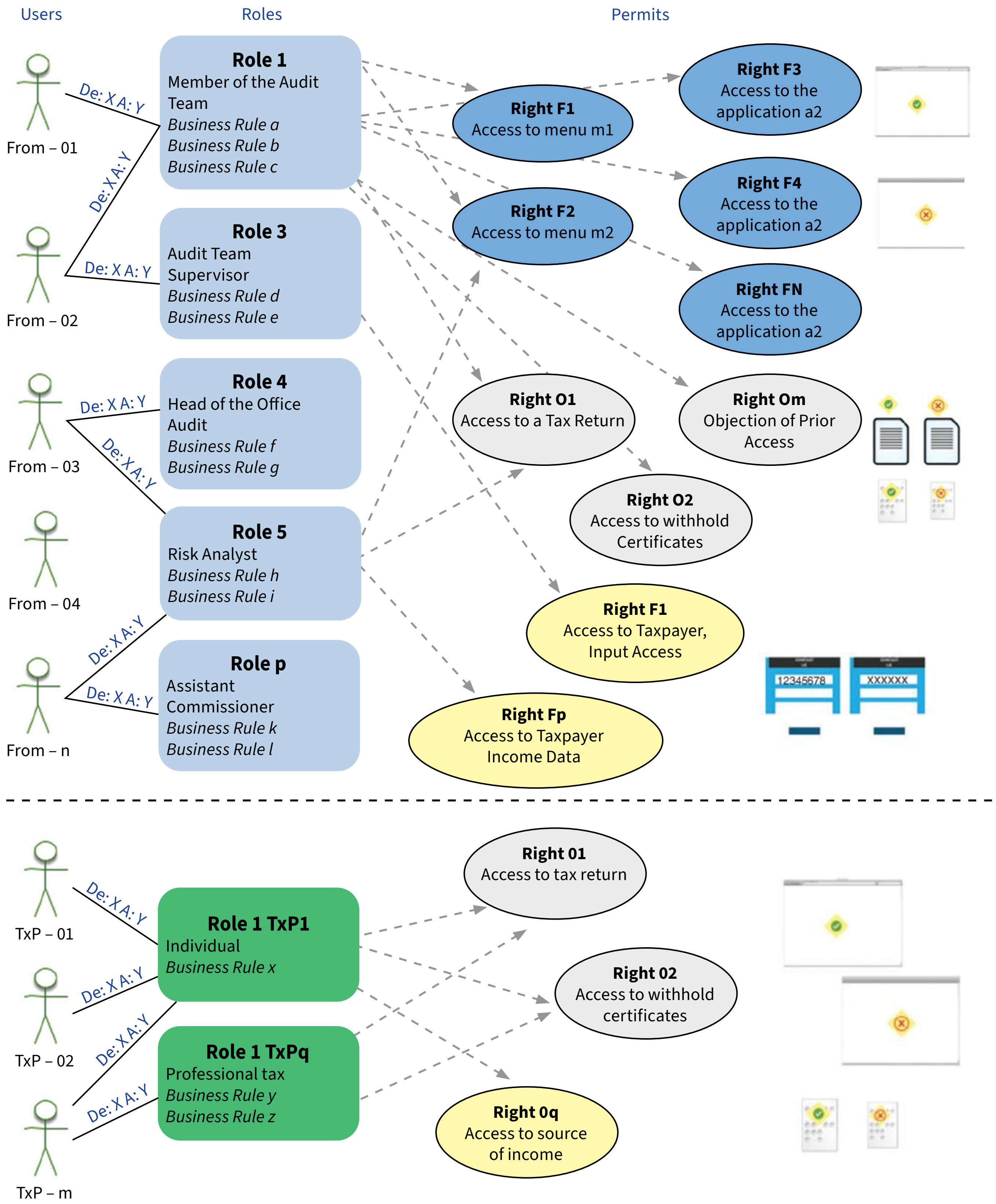
a) **Functional level**: This permission would grant access to the functional parts of the system, limiting access only to certain users.

b) **Object level**: Type of access limited exclusively to certain types of objects for a specific time or for the performance of a specific task, such as an audit.

c) **Field level**: Allows access to specific fields of an object.

The following diagram illustrates a security framework within an information system in which access is granted according to specific roles and for limited periods of time.

[41] CIAT, *ICT as a Strategic Tool to Enhance the Efficiency of Tax Administrations, Panama*, 2020, pages 352–353. Full document available at: https://www.ciat.org/Biblioteca/Estudios/2020_TIC-CIAT-FBMG.pdf



Source: CIAT (2020)

Subsequently, specific policies must be designed to establish the basic criteria applicable to cases such as the hiring of new personnel, changes, increase or reduction of functions, temporary or permanent withdrawal of employees, temporary or reduced access, privileges and restrictions, blocking, elimination of access, among others.

In addition, the administration must establish processes for the review and verification of the validity of the assigned controls; this means that they must be executed where it is periodically verified that the holders of the access rights are indeed legitimate and current users and therefore it is indispensable or necessary that they continue to have the right to have such access.

Physical Access Controls

These refer to measures designed to protect physical access to the tax administration's facilities, equipment and resources. These measures must be "articulated through one or more physical security policies endorsed by senior management. These policies should include a structured set of physical security controls to be implemented within the tax administration. To ensure that these controls meet best practice standards, they should be risk-based and linked to physical design considerations and user requirements."[42]

The following are among the measures most frequently implemented by tax administrations:

a) **Physical restriction** of entry to specific areas within the tax administration facilities through the use of electronic or physical locks on doors and accesses.

b) Incorporation of identification cards, **access cards** or similar electronic devices that will allow access to restricted areas to specifically authorized personnel.

c) Installation of **security and video surveillance systems** to monitor sensitive areas and detect intrusions.

d) **Biometric access** (fingerprint readers, facial recognition or others) as a measure to verify the identity of individuals before allowing them physical access to the tax administration facilities.

[42] OECD, Confidentiality and Information Security Management Toolkit, Op Cit., pages 40–41.

Logic Access Controls

Similar to physical access controls, logical access controls are based on the principles of need-to-know and minimum privilege. However, these controls are based on the implementation of security measures designed to protect computer systems, applications and electronic data against unauthorized access. The effective granting of access will enable tax administration personnel to acquire in a timely manner the legitimate rights they need to perform their duties.

Taking into consideration that data may be stored in different locations (data centers in the tax administration's physical facilities or in external areas or in the cloud or even in environments outside the work environment), logical access controls should be adapted to such circumstances.

The administration should also implement procedures related to:

a) **User identification**: Measures focused on corroborating which users legitimately and validly have an access right.

b) **Authentication**: Irrefutable confirmation of the user's identity once he/she accesses the tax administration's IT systems.

c) **Authorization**: After authentication, the user shall be authorized to access the resources, subject to the limitations provided for by the need-to-know and minimum privilege principles.

d) **Secondary management**: management of passwords, sessions, identification of active and inactive accounts, among others.

5.3. Technological Infrastructure Security

This stage of the ITSM framework refers to the integration of IT security and its alignment with the business. This requires, in the first place, that the tax administration establishes a unit or department focused on IT management and its correct integration with the tax administration processes.

To this end, tax administrations should implement measures focused on integrating security as part of service delivery through the implementation of adequate security controls and effective management of their IT assets and service delivery by their suppliers and ensure continuity of IT services and resilience to failures.

Regulatory implementation of the Information Technology Management Unit in the Tax Administration. Costa Rica.

Organizational Structure of the Directorate of Information and Communication Technology No. 37859-H

***Article 4º** – For the fulfillment of its objective, the Directorate of Information and Communication Technologies is formed by:*

Directorate, which includes the Management, the Deputy Management, and a Secretarial Pool.
Department of ICT Infrastructure.
Department of Information Systems.
Department of ICT Services.
Department of ICT Control and Assurance.
ICT Strategy Unit
ICT Project Management Unit.

***Article 7º** – To fulfill its functions, the ICT Infrastructure Department will be made up of five units.*

Network and Communication Management
Servers Management
Micros Management
CIT Operations Management.
Database Management.

***Article 8º**- Objective: To provide an updated and robust technological platform that ensures the efficiency, availability, and continuity of Information and Communication Technology services.*

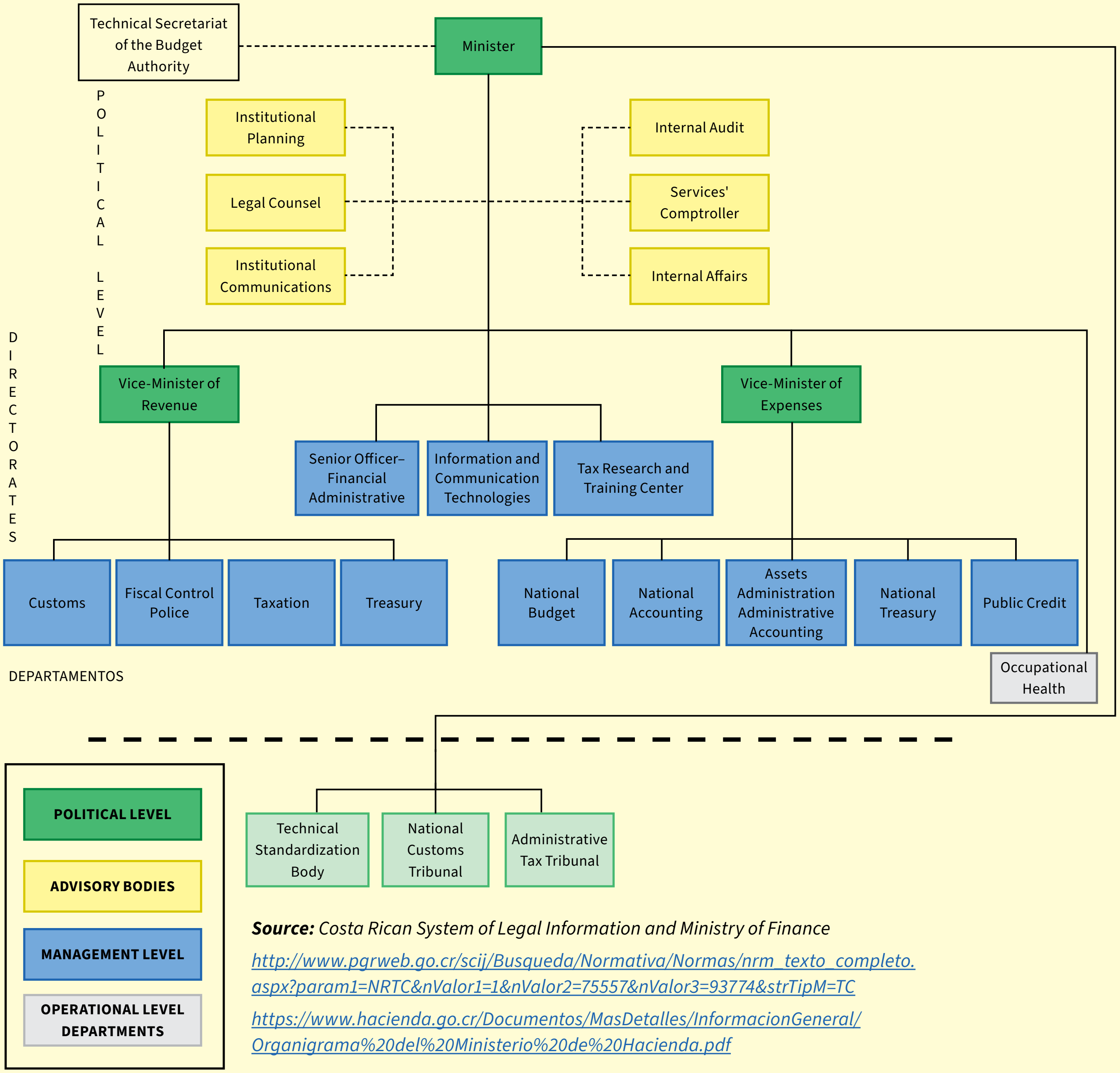
***Article 9º** – To fulfill its objective, the ICT Infrastructure Department will have the following functions.*

Propose to management the policies, procedures, and methods related to the administration of the infrastructure.
Ensure an updated and robust technology platform that supports the availability and continuity of ICT services.
Conduct studies and research on infrastructure, for the implementation of new solutions that strengthen it.
Advise various internal and external bodies of the Institution on aspects of technological infrastructure.
Provide the necessary inputs to create and maintain a TIC information model through a solid and updated TIC architecture.

Submit reports to the Management according to their area of competence.

Comply with the Internal Control provisions established by the Directorate of Information and Communication Technologies.

Below is the organizational chart of the Ministry of Finance of Costa Rica.


Technical Secretariat of the Budget Authority
Minister
POLITICAL LEVEL
Institutional Planning
Legal Counsel
Institutional Communications
Internal Audit
Services' Comptroller
Internal Affairs
DIRECTORATES
Vice-Minister of Revenue
Vice-Minister of Expenses
Senior Officer– Financial Administrative
Information and Communication Technologies
Tax Research and Training Center
Customs
Fiscal Control Police
Taxation
Treasury
National Budget
National Accounting
Assets Administration Administrative Accounting
National Treasury
Public Credit
Occupational Health
DEPARTAMENTOS
Technical Standardization Body
National Customs Tribunal
Administrative Tax Tribunal
🟩 POLITICAL LEVEL
🟨 ADVISORY BODIES
🟦 MANAGEMENT LEVEL
⬜ OPERATIONAL LEVEL DEPARTMENTS

Source: *Costa Rican System of Legal Information and Ministry of Finance*

http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=75557&nValor3=93774&strTipM=TC

https://www.hacienda.go.cr/Documentos/MasDetalles/InformacionGeneral/Organigrama%20del%20Ministerio%20de%20Hacienda.pdf

Implementing Security Controls

However, in connection with the implementation of adequate security controls, it is necessary for management to carry out a risk assessment that determines the specific risks faced by management and also identifies the residual risks to management.

Based on the results of the aforementioned assessments, management will determine the type of controls it will need to implement; these are classified into three categories (basic, additional and enhanced) and can be implemented through administrative (policies, processes), physical (fences, lighting systems) or technical (firewalls, software) measures as described below:

IT Security Controls[43]		
Basic controls	**Additional controls**	**Reinforced controls**
Minimum essential controls applied as a result of the identification of specific risks carried out by the tax administration, **regardless of their severity.**	Additional measures to the basic controls implemented to mitigate the risks identified, based on the level of severity assigned to them. The type of control measure adopted will be determined **according to the risk tolerance** that the tax administration has.	Controls that help **address advanced threats,** such as technologies to detect and prevent data exfiltration.
Antivirus, logs, CCTV, password policies.	Multi-factor authentication, cheating, training and awareness policies.	Data Loss Prevention Systems, Data Centers, Encryption Policies.

Once the appropriate controls have been implemented, it is advisable for the tax administration to carry out tests to measure their effectiveness and detect in a timely manner any adjustments and modifications required in order to preserve the security of its processes. Among the measures that can be taken to assess the effectiveness of controls are key performance indicators, penetration tests, vulnerability assessments or tests with data sets.

[43] Ibidem, pages 51–52.

Secondary Management

a) **Asset and service management**: This refers to the monitoring and control of all IT assets (hardware/software) in order to optimize their use and ensure their availability and security.

As for services, the objective is to align them with the government's objectives and improve the efficiency and effectiveness of the services provided by the administration.

With the proper implementation of this management framework, costs will potentially be reduced by making the use of licenses and other assets more efficient, increasing transparency and control, optimizing and making IT services more efficient.

b) **Service level management**: "Refers to the overall relationships between the divisions of the tax business that require IT services and the entities with overall responsibility for providing those IT services."[44]

Service level management comprises two types of instruments:

- *Operational Level Agreements*: internal agreements applicable when the service depends on another department to function properly.
- *Framework Contracts*: Applicable where IT services depend on services provided by a contractor.

c) **Service provision management by the supplier**: Applicable to ensure the safety of management processes through the use of subcontracting and supply chains with its suppliers.

Recommended measures include careful evaluation and selection of suppliers, application of appropriate security clauses, implementation of monitoring and periodic auditing mechanisms to supervise suppliers' security practices, evaluation and measurement of responsiveness and resilience to potential threats, etc.

5.4. Information Protection

This stage refers to the implementation of various measures focused on protecting the information held by the tax administrations; generally, specific controls will be applied according to the phase of the information cycle in which the information is found and the classification assigned by the authority.

[44] Ibidem, page 56.

Based on the above, the tax administration must identify the types of information in its possession and, on that basis, apply control and management measures in the form of policies.

A commonly used classification is as follows:

Applicable Criteria for the Information Lifecycle[45]	
Identifying and classifying information	**Classification examples:** • *Sensitivity:* Public, internal, reserved and confidential information. • *Restriction:* Principle of need to know focused on the type of user to whom access will be granted. • *Impact of the information:* In the event that security is breached, the impact that such breach would have on the tax administration will be assessed.
Controls During the Use of the Information	**Type of information:** • *Type of Information:* Physical (printed) or digital. • *Use:* At rest (stored) or in use. **Applicable Restrictions:** • Access restrictions, data encryption, restrictions on printing, transmission and storage.
Applicable controls for information that is no longer needed	Destruction as a security measure against threats. Establishment of precise retention and conservation periods and design of specific policies.

Knowledge of the information life cycle allows the tax authority to identify the specific risks and threats to which the information is exposed. Based on this, it is possible to implement appropriate controls for each stage of the life cycle, preventing or mitigating risks such as leaks, unauthorized access and avoiding breaches that result in the loss of information or affect the privacy and security of the information held by the tax authority.

[45] Ibidem, pages 51–52.

5.5. Operations Management

This phase of the cycle focuses on the operational arrangements that tax administrations use to verify that the ISM system and its controls are working. For such purposes, it is required to implement additional controls applicable in different areas of operational management. Among the most important are:

Log Management

A core point in the implementation of the ISM framework is the adoption of measures, practices and policies focused on ensuring that information and systems are adequately protected throughout their life cycle.

In this regard, the implementation of procedures for the creation, storage, access and disposal of records in accordance with security and confidentiality standards must at all times be aligned with the comprehensive policies of the tax administration and, in addition, requires the application of technologies and tools that allow the automation of the management of such records, including the capture, classification, storage and retrieval of information.

It is also necessary for the tax administration to implement records management systems that are interoperable with other tools and information security systems that already exist within the organization.

Records may be classified into three main categories:

a) **Security logs**: These logs are essential for auditing and analyzing events related to information security. They document activities related to authentication mechanisms, access control and potential security events. Their purpose is to facilitate the identification of unauthorized access attempts, unusual user behavior patterns and possible security incidents, enabling timely detection and response to threats and vulnerabilities.

b) **Application logs**: Designed to capture specific events and activities at the application level. They include detailed information on user interactions, errors, warnings and performance metrics. These logs are fundamental for troubleshooting and diagnosing operational anomalies within applications, providing critical data for performance optimization and identification of functional failures.

c) **System Logs**: These provide a detailed view of the operation of the operating system and its underlying components. They include data on system configurations, resource utilization and hardware events. These logs are crucial for continuous monitoring of the health and performance of tax administration systems, enabling proactive detection of infrastructure problems and facilitating efficient management of system resources.

In general, log management is an important component in the implementation of the ISM framework as it is useful to assist in the identification of security incidents, policy offenses, fraudulent activities and to provide information that could be critical for timely incident response.

The logs will also provide information that will be useful for auditing and forensic analysis, supporting internal management investigations, establishing baselines, and identifying operational trends and long-term issues.

Vulnerabilities Management

Vulnerability management is a fundamental practice to ensure the security of the tax administration's systems, tools and applications, which involves the identification, assessment, treatment and constant monitoring of vulnerabilities that may be exploited by external or internal threats and its objective is to reduce the risks associated with these vulnerabilities, ensuring the protection of the organization's information assets.

Vulnerability management must be a continuous process and intrinsically integrated into the organizational culture. This involves the systematic repetition of the process to ensure that it adapts to the changing dynamics of the IT environment ensuring a proactive stance in protecting your systems and data against potential attacks and exposures, facilitating agile adaptation to emerging threats and mitigations.

One of the most commonly implemented measures as part of the vulnerability management framework is **the penetration test** (pentest), which consists, broadly speaking, in the application of security tests that launch simulated cyber-attacks with the sole purpose of finding vulnerabilities in the tax administration systems.

Once these tests have been executed, the tax authority must document the exploitable vulnerabilities that affect the security and confidentiality of the information in order to carry out an investigation and analysis that will allow it to subsequently issue recommendations for mitigation, suggest procedures to help minimize the impact or define corrective actions to eliminate the detected flaws and finally, to verify their effectiveness by repeating the penetration test or by executing follow-up measures.

Incident Management

The tax administration must design and implement processes for the identification and management of incidents that are executed regularly and effectively. This implies that policies, processes, and procedures aimed exclusively at the detection, attention, and timely resolution of security and confidentiality events or violations are developed.

In general, the incident management process begins with the **detection or identification** of the incident (whether it is a security breach, confidentiality violation or any other similar event that may affect the security of the information held by the tax authority).

Once identified, the incident will be subjected to an evaluation in which it will be analyzed, categorized, prioritized and prepared for attention while, on the other hand, management must conduct an **investigation** of the incident to determine and evaluate its impact. Once this analysis has been completed, **specific actions** shall be taken to respond to or address the incident until its **final resolution**.

Managing Changes

It refers to "the controlled management of the development of new systems and services, as well as the implementation of major changes to existing ones. It includes the design of robust solutions, testing and release control, and is the means by which it is ensured that IT security is incorporated into system changes."[46]

The core point of the execution of the change management process is that it is considered a high-risk measure since, if carried out in an uncontrolled manner, there is a high possibility that the confidentiality, integrity and availability of the tax administration's systems may be jeopardized.

Tax administrations must implement the change management method that best suits their requirements, circumstances and needs and keep it, at all times, aligned with the comprehensive policies on information security and confidentiality.

[46] Ibidem, page 89.

6. Monitoring and Prevention

Practices related to monitoring and prevention are essential for tax administrations as they allow them to detect and respond in a timely and proactive manner to possible threats, reduce potential security breaches and minimize the impact of any attacks that may occur.

One of the most effective measures to monitor and prevent cybersecurity breaches is the constant review of controls in technological systems, processes and procedures. Periodic evaluation of these controls strengthens the tax administration’s defenses against external and internal threats and guarantees the effectiveness of the measures implemented.

The implementation of monitoring and prevention measures helps to protect the IT infrastructure of tax administrations against malicious attacks. These measures act as an additional barrier against external threats.

Thus, measures such as the establishment of clear parameters, the continuous review of controls, the execution of tests and evaluations and the generation of detailed reports and the performance of internal or external audits will allow the tax authority to implement improvement actions, thus contributing to the adoption of an effective security strategy that will ensure not only the protection of sensitive data, but also compliance with regulations and confidence in the integrity of the tax administration systems.

6.1. Definition of Parameters

The monitoring and prevention phase begins with the clear definition of security parameters, i.e., the tax administration must establish and specify criteria, limits or guidelines that guide the implementation and operation of security controls. These parameters are essential to ensure that security measures are effective and consistent within the administration and must always be aligned with national and international regulations applicable to information security in tax matters.

To this end, it is necessary to identify which systems and applications will be monitored and then establish specific thresholds to set security alerts (volume of transactions, failed access attempts to applications, etc.), and finally, as part of the protocol, clear policies must be defined regarding the applicable procedures for the periodic review of security systems.

These parameters will serve as indicators for the authority to carry out review and evaluation procedures and obtain useful information regarding the state of its systems in terms of cybersecurity.

6.2. Controls Review

The purpose of the controls review stage is to evaluate and verify the effectiveness of the security controls implemented, as well as to identify areas that need to be adjusted and/or improved to strengthen the ISM and ITSM framework. This implies that the tax administration should adopt a system that verifies that the controls foreseen in the policies are adequately and effectively implemented.

The review of internal and external controls to monitor information security is a continuous and multidimensional process as it requires a combination of technical controls, organizational policies and inter-agency collaboration to protect information and, consequently, ensure public confidence in the tax system.

In this regard, the OECD notes 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. 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 about operations management, but also based on lessons learned from specific breaches."[47]

This phase is transcendental since it allows the tax administration to validate the effectiveness of the implemented measures and adapt them as required. In the medium term, the organization will have the certainty that it remains aligned with current security standards and proactively address cybersecurity threats while improving the perception of confidence in the organization's ability to manage and protect information securely and effectively.

In addition to the internal controls mentioned above, tax authorities should establish robust external control mechanisms through the implementation of measures such as independent audits, obtaining certifications from regulatory bodies or even collaborating with other tax authorities -for example, through the exchange of information.

[47] OECD, Confidentiality and Information Security Management Toolkit, Op. Cit., pages 98–99.

Through such actions it will be possible to evaluate the effectiveness of internal controls and obtain recommendations and/or best practices to improve the security of tax information. These reviews, in addition to validating the effectiveness of internal controls, will also allow for the timely identification of potential vulnerabilities or weaknesses that could be unduly affected by internal or external threats or risks.

6.3. Tests and Evaluations

IT security testing is essential to simulate attacks and evaluate the responsiveness of systems to different scenarios. These tests provide valuable information to improve resilience and recovery capacity in the event of possible incidents.

In general, in this phase the tax administration should apply technical and non-technical assessments to qualify the security and confidentiality of the information in the jurisdictions or entities subject to the diagnosis. This may include vulnerability analysis, penetration testing, review of policies and procedures, interviews with key personnel and review of relevant documentation.

Compliance Audits

An effective measure to adequately assess the effectiveness of the implementation of the ISM framework can be the execution of an **audit** through which the tax administration will be able to ensure that it complies with information security and confidentiality regulations. Through this procedure, it will be possible to identify, evaluate and mitigate cybersecurity risks in a timely manner.

Audits can be executed *internally* (if carried out by the tax administration's own staff) or *externally* (performed by a third party expert in the field); regardless of the approach, it is necessary for the auditor to have a clear and comprehensive understanding of the organization, its objectives, risks and processes in order to fully address the cybersecurity challenges faced by the tax authority.

Items that Can be Analyzed During an Audit[48]	
Technical Assessment	
Operations and Technology	• Vulnerability scanning and penetration testing • Network logging and monitoring/ threat assessment • Device configuration reviews (infrastructure, firewalls, routers, etc.) • Wi-Fi: Scanning for unauthorized Wi-Fi/ and Wi-Fi configurations and vulnerability/ exploitation teesting • Remote Access /VPN Points: Technical assessment of remote access points and configuration to help ensure their protection • Application/database assessment, to carry out vulnerability scanning, penetration testing, and database configuration • Security by Design • Architecture reviews and analysis • Operating system/database security settings • Patching process/remediation procedures • Code review.
Process and Control Assessments	
	• Identity and access management. • Access management procedures. • Remote access management and authentication. • Privileged access management. • Physical and personal security: Logical and physical access controls, security/social engineering awareness, and mobile device security. • Operations security assessments.
Human Factors	• Talent management and IT training.
Leadership and Governance	• Cybersecurity governance, roles and responsibilities. • Integration of cyber and business risk management.
Legal and Compliance	• Regulatory considerations and integration into the cyber framework.
Information Risk Management	• Supplier risk management and security. • Cyber Threat Analysis and Risk Management Process: Threat identification, assessment, and update process, including integration with change management and software development lifecycle. • Cloud IT security and continuous assessment. • Data classification, protection and encryption, training and awareness programs across the organization.

[48] KPMG, "*The role of internal audit in cyber security readiness*", 2019. Document available at https://assets.kpmg.com/content/dam/kpmg/lu/pdf/2019/lu-en-cyber-databreach-brochure.pdf

6.4. Reports

Security reports provide a comprehensive view of the state of cybersecurity within tax administrations. These reports are critical to making informed decisions and effectively allocating resources to mitigate risks.

6.5. Implementation of Improvement Actions

The implementation of improvement actions based on the results of tests and evaluations contributes to strengthening the technological security of tax administrations. These actions may refer to software upgrades, staff training and the implementation of stricter security policies.

Based on the tax administration's analysis of the information gathered during the review phase (i.e. evaluations, tests, audits, reports), the authority will be able to identify the areas where changes, adjustments and improvements are required. Subsequently, an action plan should be designed to address the areas of opportunity that need to be addressed, prioritizing actions based on their impact and urgency. Finally, the planned improvement actions should be implemented and tested to verify that they are working properly.

Raising staff awareness of cybersecurity best practices is essential to reduce the possibility of potential insider attacks and human error. Regular training on the importance of maintaining secure passwords, identifying malicious emails and protecting confidential information helps to strengthen the security posture of the tax administration.

Likewise, investment in advanced security technologies and the constant updating of systems are necessary to keep up with the various technological threats that are increasing exponentially. Continued commitment to improving cybersecurity is essential to protect the information held by tax authorities and thus ensure confidence in tax administration systems.

OECD recommendations to ensure the security and confidentiality of information.

The following recommendations have been created to help tax authorities ensure that taxpayer confidential information is properly safeguarded.

(…)

- *There will be comprehensive policies and procedures regarding the confidentiality of tax information, which must be regularly reviewed and endorsed at the highest level of tax administration. Moreover, it must be clear who is responsible for implementing the policy within the administration.*
- *All individuals who have access to confidential information must undergo background checks or security screenings.*
- *The employment contract or employment agreement must include provisions relating to the employee's obligations regarding the confidentiality of tax information, and furthermore, such obligations shall not cease once the employment relationship has ended. Consultants, service providers, and contractors shall be contractually obligated to comply with the same obligations as employees (whether full-time or temporary) and such obligations shall prevail beyond the contract or collaboration period.*
- *Employers must provide training and regular reminders explaining the employee's responsibilities regarding confidential tax information, clearly determining where they can seek help if they have questions or need advice.*
- *The areas, or zones within the facilities, where the tax information is located must be secure and not accessible by unauthorized persons.*
- *All situations of storage, circulation, access or disposal of documents containing confidential information (both in paper and electronic format) must be carried out securely and ensuring the confidentiality of the documents.*
- *Policies and procedures for managing disclosures of confidential information made without authorization must be in place.*
- *All information requests and all information received must be securely filed. Access will be strictly controlled and actions will be taken according to the principle of "need to know."*

Source: *Keeping it Safe. The OECD Guide on the Protection of Confidentiality of Information Exchanged for Tax Purposes.*

7. Generation of Open Data in Tax Administrations

7.1. Definition

The OECD defines open government as "the governance culture based on innovative policies and sustainable public policies and practices inspired by the principles of transparency, accountability, and stakeholder participation in support of democracy and inclusive growth," while an Open State occurs "when the executive, legislative, and judicial powers, independent public institutions, and all levels of government – recognizing their respective roles, prerogatives, and general independence according to their current legal and institutional frameworks – collaborate, exploit synergies, and share good practices and lessons learned among themselves and with other stakeholders to promote transparency, integrity, accountability, and stakeholder participation, in support of democracy and inclusive growth."[49]

Recently, the importance and impact of open data in relation to sustainable development goals has been recognized, as it is considered to have the potential to transform the way governments address global challenges, providing valuable information for decision-making and promoting transparency, participation, and innovation. Governments around the world have launched initiatives[50] that not only promote the disclosure and effective use of public data but have also set large-scale goals such as sustainable economic growth, combating climate change, gender equality, and poverty reduction, among others.

In 2024, the OECD published in the study titled Public Administration Outlook: Latin America and the Caribbean 2024[51] – in chapter 9 related to Digital Government and Open Government Data – the results of the

[49] OECD Council Recommendation on Open Government. Available at https://www.oecd.org/gov/oecd-recommendation-of-the-council-on-open-government-es.pdf

[50] Open Data for Development. More information is available at https://www.od4d.net/

[51] OECD (2024), Public Administration Overview: Latin America and the Caribbean 2024, OECD Publishing, Paris, p. 128. Document available at https://doi.org/10.1787/0f191dcb-es.

Open, Useful, and Reusable Data Index (OURdata) [52]. This index evaluates three fundamental pillars regarding open government data.

b) Availability of open data: Analyzes the degree of adoption and implementation of various requirements for the publication or dissemination of governmental open data. It also assesses the demand for such data and the available datasets.

c) Accessibility of data: Refers to the established requirements for providing data in suitable and high-quality formats, including the medium through which it is supplied. It also evaluates the degree of stakeholder engagement.

d) Data reuse: Analyzes the degree of government support and proactive promotion for the reuse of information.

In relation to this assessment, the Index revealed that, regarding the six countries[53] in Latin America and the Caribbean included in the analysis, on average, they scored below the OECD[54] average in the three pillars of the index, which allows us to conclude that there are still areas where it is necessary to adopt and implement more effective measures and policies that promote and facilitate access to public information in a quick, simple, and appropriate manner.

7.2. Legal Framework of Open Data Governance

Based on the above, one of the fundamental elements upon which the effectiveness of implementing open data policies depends is the existence of a robust legal framework that includes policies, standards, and regulations that ensure the availability and accessibility of information by establishing the limits, rights, and obligations for both the authority and the citizens.

In general, there are various ways in which policies related to governmental open data can be implemented or adopted; what is crucial is that these policies are incorporated into the domestic legislation of the jurisdictions in order to provide legal certainty to both citizens and the administrations themselves regarding

[52] OURdata is a survey that seeks to evaluate the efforts of public administrations related to the design and implementation of domestic government open data policies.

[53] Brazil, Chile, Colombia, Costa Rica, Mexico, Peru.

[54] The assigned score of each pillar has a value of 0 to 1, the total score assigned corresponds to an average of the grades of the three (3) pillars. In this case, the countries of Latin America and the Caribbean obtained an average score of 0.37; the average score for OECD countries was 0.48.

how governmental openness will be carried out. Basic guiding principles must be established, and the scope and restrictions on access to information must be clearly delineated, including the obligated subjects and all applicable procedural norms, particularly those concerning the time and format in which the information will be disclosed.

Based on the above, open data policies can be contained in various instruments or normative bodies.:

a) **National Constitution**. Several jurisdictions have elevated the explicit recognition of the right to access information to constitutional status. From this, specific laws and secondary regulations would be developed. This is the case of Guatemala, Mexico, Panama, countries that also have specialized regulations on transparency and access to information.

Explicit recognition of the right to access information at the Constitutional level. Panama.

ARTICLE 43.

Every person has the right to request public access information or information of collective interest that resides in databases or records held by public servers or private individuals providing public services, as long as that access has not been limited by written provision and by mandate of the Law, as well as to demand its fair treatment and correction.

ARTICLE 44.

Every person may promote a habeas data action seeking to guarantee the right of access to their personal information collected in official or private databases or records, when the latter involve companies that provide a service to the public or are engaged in supplying information.

This action may also be taken to enforce the right to access public information or free access, in accordance with what is established in this Constitution.

Through the action of habeas data, it is possible to request the correction, update, rectification, suppression, or maintenance of confidentiality of information or data that are personal in nature. The law will regulate those matters concerning the competent courts to hear habeas data cases, which will be processed summarily and without the need for a legal representative.

b) **Specific laws on transparency and/or access to information.** These regulations are the core of open government policies. The approach adopted by most jurisdictions is to implement regulations that address both transparency and access to information, regardless of whether there is an explicit recognition of the right to access information at the constitutional level. This includes countries such as Argentina, Colombia, Spain, Honduras, Guatemala, Mexico, among others.

c) **Secondary regulations.** Primarily administrative regulations, rules, guidelines, circulars, etc. Related to procedural issues, internal administrative regulations, information management, among other issues.

7.3. Minimum Elements of the Regulations on Transparency and Access to Information

In general terms, regardless of the legal instrument used for its implementation, the regulations regarding transparency and access to information must include, at a minimum, the following elements:

Object: Refers to indicating the general purpose of the regulation, which is to guarantee access to information in the possession, custody, or control of authorities or obligated subjects. It is based on the principle of maximum publicity, which states that any information in the possession of authorities must meet three attributes: completeness, timeliness, and accessibility.

Obligated subjects: As a general rule, these are considered to be institutions of Public Administration at the central or federal, regional, provincial, or municipal levels, and decentralized and deconcentrated bodies.

Requesting subjects: Any person will have guaranteed access to submit requests for information, even anonymously, without justifying the reasons for the information request.

Active Disclosure: The obligated subject will proactively disseminate information without any request; the regulations must specify which information will be subject to proactive disclosure, for example, information about public officials, budgets, financial management, public works, public spending, etc.

Obligations: The primary and additional obligations that obligated subjects must comply with when handling information requests should be described.

Special cases: Special or specific situations may be incorporated, directed at specific sectors or regarding types of specialized or specific information.

Procedures applicable to information requests: The assumptions under which citizens may request information must be clearly described. The regulations must cover, at a minimum, the applicable requirements, processing, notification procedures, time and manner of delivery, inherent costs to the request (even though the process must be free, it is possible that the citizen may require a format that could be charged, such as certified copies), response periods, means and resources for appeal or contestation.

Exceptions: Clearly and precisely indicate the circumstances under which obligated subjects may validly deny access to information. Generally, exceptions relate to reserved information (excluded due to a clear, probable, and specific risk of harm to public interests) or *confidential information*.

Actions on active transparency. Costa Rica

Decree No. 40200-MP-MEIC-MC

Article 11. *Decentralized public institutions will seek to publish at least the following public information on their respective official websites.:*

Normative framework governing the public management of the institution.
Organizational structure, competencies, obligations, and services provided.
Institutional directory.
List of institutional officials.
Institution's hours of operation.
Detailed description of the services provided to the public and the way these are carried out.
Institutional plans and budgets, as well as their execution and evaluation methods.
Processes for recruitment and selection of personnel.
Mechanisms and results of the performance evaluation process of officials.
Payrolls with the gross salary.
Annual operational plan and strategic plans.
Annual reports and other management reports.
Internal Audit Reports on institutional management.
Minutes of the collegiate bodies established by law, except by express legal provision.
Clear and precise description of the procedures and requirements that can be carried out before the institution.
All information on the stages of the administrative contracting processes of the institution.
Mechanisms for submitting requests for information, petitions, complaints, and suggestions for the improvement of the institution's functions, as well as any other means of citizen participation.
List of subsidies, grants, donations, exemptions, or any other transfer or benefit granted to individuals, without prejudice to what is determined in the Law on the Protection of the Person Against the Processing of Personal Data, regulation number 8968.
Travel reports, representation expenses, travel costs, payments for travel allowances of the institution's officials, among others.
Any other information that promotes transparency and control in the exercise of public function.
The publication of this information related to the management of each institution will be in an open, interoperable, and accessible format.

Classification of information: The categories applicable to the information held by the authorities and the procedures for carrying out classification and declassification must be clearly regulated.

Journalism and access to information. Honduras.

In Honduras the Law on Transparency and Access to Public Information (Decree 170–2006), there is a legal assumption that guarantees journalists access to information. This represents a special case within the regulatory framework related to issues of transparency and access to information since, in the first instance, it is specifically aimed at the journalistic sector and in the second instance because, indirectly, it facilitates and safeguards the right of access to information of the citizens as a whole

This provision is transcribed below:

Article 22. Access to Information by Journalists. The authorities are obliged to give protection and support to journalists in the exercise of their profession, providing them with the information requested without any restrictions other than those contemplated in this law and other laws of the Republic.

Specialized bodies: Bodies can be established that will be responsible for promoting, ensuring, and monitoring compliance with the obligations related to access to information.

Creation of regulatory bodies for transparency. Panama

Panama has specific legislation whose main objective is the creation of a body to regulate and monitor compliance with access to information obligations.

Law 33 of April 25, 2013 creating the National Authority for Transparency and Access to Information

Article 1. The National Authority for Transparency and Access to Information, hereinafter referred to as the Authority, is hereby created as a public, decentralized institution of the State, which shall act with full functional, administrative and independent autonomy in the exercise of its functions, without receiving instructions from any authority, State body or person. (…)

Article 2. The Authority shall ensure compliance with the rights enshrined in the Political Constitution of the Republic of Panama regarding the Constitutional Right to petition and access to information, as well as the rights set forth in the conventions, agreements, treaties, international and national programs on the prevention of corruption and the insertion and implementation of new prevention policies in public management at the governmental level on its own initiative or by national or international proposals.

Infractions and sanctions applicable in cases of non-compliance and violations of transparency obligations.

Sanctions for non-compliance with transparency obligations. Dominican Republic

General Law of Free Access to Public Information, No. 200–04.

Criminal and Administrative Penalties Impeding or Obstructing Access to Information

Article 30. The public official or responsible agent who arbitrarily denies, obstructs or impedes the applicant's access to the requested information shall be punished with imprisonment from six months to two years, as well as disqualification from holding public office for five years.

7.4. International Scope

Open Government Partnership

In the international arena, there is an initiative that aims to provide an international platform that seeks to incorporate governments, civil society, and citizens in order to ensure access to information and accountability.

This initiative, launched in 2011, is known as the Open Government Partnership and to date includes 75 countries[55], 150 local governments (state and/or municipal), and multiple civil society organizations.

To join the Partnership, governments are required to meet basic eligibility criteria. These criteria evaluate four distinct areas: fiscal transparency, access to information, disclosure of public officials' assets, and citizen participation. Additionally, a values verification assessment will be applied, focusing on the interaction between governments and civil society organizations, primarily the control of their entry and exit from public life and the extent to which the government seeks to suppress them.

[55] In the case of the **Americas**, the member countries – as of this date – are: Argentina, Brazil, Canada, Chile, Colombia, Costa Rica, Dominican Republic, Ecuador, Guatemala, Honduras, Jamaica, Mexico, Panama, Paraguay, Peru, the United States and Uruguay. El Salvador was a member for the period from 2011 to 2023, currently its status in the Partnership appears as *withdrawn*.

Finally, governments must support the *Open Government Declaration*[56] through which they will reaffirm their commitment to the principles of open and transparent government by designing and implementing an action plan through public consultation and annual self-assessment reports regarding the relevance of the basic principles of open government and the implementation of the Action Plan.

Now, for the period 2023 – 2028, the Partnership has designed a global strategy that revolves around five fundamental objectives that must be implemented according to the capacities and conditions of each member. These objectives are:

a) To form an ever-growing, committed, and interconnected community of reformers, activists, and leaders of open government.

b) To make open government fundamental to the operation and priorities of governments at all levels and branches.

c) To protect and expand civic space.

d) To accelerate collective progress in favor of open government reforms.

e) To be a center for innovative cases, evidence, and inspiring stories of open government.

The Partnership has a review mechanism to assess the status of the implementation of the Action Plans designed by the member governments. This mechanism, known as the Independent Review Mechanism, consists of a multinational group of experts who evaluate the level of progress in implementation.

The results of the review are published in reports that reflect the level of progress in terms of transparency, accountability, and citizen participation of the action plans, and also contain technical recommendations to guide the actions of the parties aimed at achieving their objectives.

Regarding the participation of jurisdictions in the region, the following stands out:

a) **Costa Rica**: Joined the Partnership in 2022 at the local level. To date, it has presented an Action Plan and has made two commitments related to local administration.

b) **Guatemala**: Joined at the national level in 2011. It has presented a total of six Action Plans – the last one submitted in 2023 – and has made 126 commitments. Among these commitments the following stand out: *Institutional actions to strengthen open data, participatory update of the digital government plan, strengthening of open data, creation and implementation of a comprehensive strategy on transparency, open government, and anti-corruption, strengthening of anti-corruption mechanisms of transparency and*

[56] Full text available at https://www.opengovpartnership.org/es/process/joining-ogp/open-government-declaration/

results that demonstrate the national and international level, and actions to continue advancing in the adoption of international controls on fiscal transparency, procurement, and contracting.

c) **Honduras**: Joined in 2011, has presented five Action Plans (the latest Plan was presented in 2023) and to date has undertaken 93 commitments. The most relevant commitments related to transparency and access to information were: *Open data, Implementation of the Transparency and Access to Public Information Law, Comprehensive policy, transparency, probity, and ethics, Ethics in public service, Respect for the citizen's right to obtain information from public records.*

d) **Panama**: Joined the Partnership in 2012, to date has presented five action plans and has assumed 48 commitments. The most relevant are: *Implementation of the Transparency Law, Institutionalization of open government in Panama, and Accountability of public institutions*.

e) **Dominican Republic**: Joined – at the local level – in 2022, assuming five commitments and 1 Action Plan.

Open Data Charter

Another relevant project in the field of open data is the Open Data Charter[57], which is a global initiative that promotes openness and transparency in the publication of data. It aims to encourage governments, organizations and companies to publish data in an open, accessible and reusable way so that society can benefit from it.

The Open Data Charter establishes fundamental principles to promote openness and effective use of government data. These principles are:

a) Access and use: Data should be available to all, without access restrictions and with clear permissions for its use.

b) Quality and quantity: Data should be accurate, timely and complete, ensuring its usefulness for various applications.

c) Transparency: Open data should promote transparency in government management and improve accountability.

d) Innovation and added value: The availability of data should foster innovation, creating economic and social value through new applications and services.

e) Participation: Citizen participation and civic engagement should be facilitated through access to relevant and understandable data.

[57] https://opendatacharter.org/principles/

Punta del Este Declaration

In 2022, the 6th Meeting of the Punta del Este Declaration was held, whose main objective is to maximize the effective use of information exchanged under the different standards of exchange of information for tax purposes. It also seeks to address tax evasion, corruption and other financial crimes through the broad use of information, the creation of effective frameworks that allow the availability and access to beneficial ownership information, the use of automatically obtained financial information, among other issues.

As a result of this meeting, the General Assembly made four recommendations:

a) *Adopt, always within its legal scope of action, an active and vanguard role in adapting society to the challenges of digital development and taking advantage of the opportunities of new technologies; by, among other measures, reinforcing the IT security of tax information and communications, establishing adequate data governance models in the digital era and implementing continuity plans for the tax administration's fundamental operations.*

b) *Establish synergies with society -companies, citizens and the rest of the State agencies and bodies- in order to promote the development of their countries and societies; collaborating internally, with full respect for privacy protection mandates, maximizing the usefulness of the accurate and fast information available to the tax administrations thanks to technological innovations and implementing a policy of open data availability, safeguarding taxpayers' privacy and using data anonymization techniques.*

c) *Contribute to promote, within the framework of its actions, social inclusion and the fight against informality; collaborating within the legal framework of each country and ensuring respect for taxpayers' rights in the proper implementation of social policies, taking advantage of the quality and quantity of information handled by the tax administrations.*

d) *Promote best practices in the development of the tax administrations' personnel in order to achieve the operating, collection and control objectives previously set.*

7.5. Available Open Data

The importance of data publication in tax administrations is mainly explained by the following reasons:

a) **Transparency and accountability**: it allows citizens and civil society organizations to monitor how public funds are collected and used, promoting a more efficient and ethical management of resources.

b) **Improved decision making**: Stakeholders from the private sector, academia, civil society among others can make more informed decisions based on up-to-date and accurate data, which can lead to more effective and equitable fiscal policies.

c) **Fostering innovation and economic development**: Open data can serve as the basis for the development of new tools and applications that simplify tax processes, improve user experience and promote voluntary compliance.

In 2022 the Open Data Barometer and Data for Development published the Global Data Barometer, with the aim of assessing the state of data worldwide, seeking to promote collective learning about effective practices and successful strategies. According to the Barometer[58], open data must meet essential requirements to ensure its effectiveness and usefulness, including being freely and unrestrictedly available, accessible to all citizens, maintaining high integrity and quality, being structured to facilitate interoperability, and promoting community participation in its use and continuous improvement.

A look at the open portals of the most advanced Tax Administrations shows that the attributes that are generally present in open data initiatives are as follows:

a) **Accessibility**: data is available in an accessible and easy-to-find manner to the general public, without significant technical or bureaucratic barriers. For example, the Canada Revenue Agency (CRA) has published 292 records on the Open Government Portal.

b) **Regular updating**: there is a commitment to regularly update data, ensuring that the information available is relevant and accurate at all times. In the specific case of Canada, of the 292 records, 251 are updated annually, 13 do not have a specific schedule for updating, 11 are updated quarterly, 11 as needed, 5 are updated monthly and 1 is updated semi-annually.

c) **Interoperable formats**: The data are provided in standard formats, which facilitates their use by developers, researchers and citizens in general. In the specific case of Canada, 98% of the records are available in CSV format, 73% are available as HTML and only 31% as PDF. In addition, 18 records are API-enabled.

d) **User feedback**: User feedback is encouraged and citizen participation in the continuous improvement of the services and information available is promoted. In the specific case of Canada, the country has a Multi-Stakeholder Forum on Open Government – Canada.ca

[58] The text is available in the following link: https://globaldatabarometer.org/wp-content/ uploads/2022/05/GDB-Report-Spanish.pdf

Multisectoral forum on open government – Canada

Established on January 24, 2018, the Multisectoral Forum on Open Government aims to (i) provide input and advice on the Government of Canada's open government commitments, (ii) identify new areas of focus, and (iii) strengthen the open government community across Canada.

The Terms of Reference of the Multisectoral Forum detail the following responsibilities and functions of the forum:

1. ***Advice on open government commitments:*** *The forum provides advice and recommendations on the specific open government commitments adopted by the Government of Canada, ensuring that they are consistent with the principles of transparency and citizen participation.*
2. ***Identification of new areas of focus:*** *In addition to reviewing current commitments, the forum is tasked with identifying emerging or priority areas where open government can be strengthened or expanded. This includes exploring new technologies and methods to improve the openness and accessibility of government data.*
3. ***Development of the open government community:*** *The forum promotes collaboration and the exchange of best practices among different stakeholders, thereby strengthening the open government community throughout Canada. This is achieved through events, workshops, and other activities designed to encourage participation and joint learning.*
4. ***Structure of members:*** *The forum is made up of a total of 12 member positions, divided into eight for representatives of civil society and four for members of the Government of Canada. This structure ensures a balanced and diverse representation of interests and perspectives related to open government.*

Source: *Canadian Government*

Open data catalog of the Spanish State Agency for Tax Administration

Some examples of open data available in Spain are the following:

1. *Advance of domestic sales in large companies and SMEs: It provides weekly data on sales made by both large and small and medium-sized enterprises (SMEs) in the Spanish domestic market. Its purpose is to offer an overview of the evolution of sales in the national market, which can be useful for analyzing economic and commercial trends.*

2. *Observatory of business margins: provides quarterly data for the monitoring and analysis of business margins, information that comes from corporate tax returns, as well as from VAT models and withholding on labor income. This data includes variables from the Profit and Loss Account of Corporate Tax, sales and purchase figures from VAT, and data on payroll and salary recipients.*

3. *Corporate and non-corporate SMEs: annual figures related to economic activities provided by entrepreneurs and individual professionals in their annual Income Tax declarations and in the information related to the financial statements that corporate entities submit in their annual Corporate Tax declarations.*

4. *Statistics of the taxpayers of the Personal Income Tax of the largest municipalities by postal code: It provides a detailed analysis of gross average income and other figures reported at the postal code level. This statistic reflects the significant disparity in average income between neighborhoods in large cities and dispersed rural areas. The selected municipalities meet at least one of the following criteria: having more than 200,000 inhabitants, receiving more than 100,000 income tax returns, or having a total gross income greater than 2.2 billion euros.*

5. *Daily sales (Weekly information SII) The statistics of the Immediate Information Supply (IIS) System (SII) provide daily data. about the sales of companies required to use this system, including Large Enterprises, VAT groups, and those registered in the Monthly Refund Registry. This system provides more up-to-date sales information than traditional monthly or quarterly VAT reports. Daily sales account for approximately 70% of the total domestic sales of VAT taxpayers. The publication includes a report and historical series since July 1, 2017, which are used to analyze the economic situation and complement other sales and tax collection reports.*

Source: *Spanish Tax Agency*

Open Data Catalog of the Canada Revenue Agency

Some examples of open data available from the Canada Revenue Agency are:

1. *T2 Statistics on Corporate Scientific Research and Experimental Development: These provide key information on tax and accounting as of March 31, 2024. The tables include selected data from all T2 corporate tax returns that were assessed or reassessed, covering fiscal years ending between 2015 and 2021. The information offers insights into the impact and implementation of tax credits.*

2. *T1 Filing Compliance, 2024 Edition: provides data on the returns that were submitted late or on time. The declarations are grouped according to demographic, geographic, and economic characteristics.*

3. *Individual Tax Statistics by Area (ITSA): They present information on personal income tax based on geographical areas. The statistics are compiled by province and territory, as well as for all of Canada. The tables provide statistics on income and taxes according to specific geographic areas, tax status classification, total income class, source of income class, and gender.*

Source: *Canada Revenue Agency*

8. Data Governance in Tax Administrations

Tax administrations have experienced a significant increase in the availability of their data, both in terms of volume and variety of formats. This increase is explained by different factors, including the digital transformation that has revolutionized data collection; the exponential growth in processing and storage capacity; the expansion of communications networks; and the generalized access to broadband Internet, among others.

Evolution of tax administrations in the OECD:

- *From 2014 to 2019, average electronic filing rates have significantly increased between 13% and 18%.*
- *Over 80% of payments (by value and number) are made electronically. Nearly 50% of tax administrations pre-fill personal income tax (PIT) returns with specific deductible expenses.*
- *The new data sources allow preloading to extend to VAT (Value Added Tax) and corporate tax (CIT) returns.*
- *A growing number of tax administrations are using virtual assistants to respond to taxpayers' inquiries and support self-service.*
- *They use artificial intelligence in services that support taxpayers and tax officials.*
- *The percentage of tax administrations that allow online registration of taxpayers has increased from 70% in 2015 to 97% in 2019.*
- *With the increasing availability of data, the focus of compliance work may shift towards prevention.*

Source: *CIAT (2022)*

In the current context of increasing volume of digital data and its recognized importance as a critical asset for decision making, strategies to manage and leverage this data in a comprehensive manner have become increasingly important. These strategies are generally referred to as data governance.

DAMA International defines data governance as “the exercise of authority and control (planning, monitoring and enforcement) over the management of data as assets” [59]. In this context, a data governance program is tasked with formulating policies and procedures that promote data management practices at all organizational levels, with the objective of optimizing the best use of data. CIAT (2022) complements this definition by stating that data governance should ensure the confidentiality, availability, quality and integrity of data, while strengthening legal frameworks for protection and compliance.[60].

Data governance can also be supported by technological tools, such as master data management (MDM) systems or business intelligence platforms, which enable better management, analysis and control of information. A prominent example is Estonia, which has implemented a data governance strategy that integrates automatic cross-checking systems between different agencies, which improves efficiency and minimizes human error.

8.1. Minimum Elements in a Data Governance Strategy for Tax Administrations (TAs)

In 2022, CIAT published in English the practical guide “Data Governance for Tax Administrations” [61], which provides a detailed framework on how administrations can achieve effective management of their data and transform themselves into data-driven organizations. The guide includes an adjustable governance model for tax administrations, designed as a starting point that can be evaluated and adapted according to the specific needs of each entity. The following section takes as a reference the key elements that CIAT recommends for a governance strategy:

a) **Principles and policies:** It discusses data governance principles that facilitate collaboration among stakeholders to achieve common goals. While each tax administration should identify the most appropriate data policies for its context, CIAT proposes the following 5 principles.

[59] Sebastian-Coleman, L. (2018) “Navigating the labyrinth: An executive guide to data management” (1st ed.). Technics Publications.

[60] Unlike data management that seeks value from these assets, data governance focuses on how decisions are made about them and how people and processes should behave in this regard.

[61] In 2024, the translation of the guide into Spanish was published and is available at the following link: https://www.ciat.org/Biblioteca/DocumentosTecnicos/Espanol/2024_gobierno_datos.pdf

Principle 1: Data as assets of the tax administration. • **Statement:** Data is a resource and asset of the tax administration. • **Justification:** The tax administration requires the use of data to ensure compliance control and design customized services. • **Implication:** Ensure the treatment and quality of data as a valuable resource throughout its cycle within the tax administration.	**Principle 2: Privacy and data protection** • **Statement:** Promote compliance with taxpayer data privacy by following laws and regulations. • **Justification:** Taxpayer and tax administration data should be treated as dictated by tax, transparency and data protection laws. • **Implication:** To ensure compliance with tax and data protection laws; data must not be used for purposes other than those specified.
Principle 3: Transparency in management • **Statement:** Data management should show transparency throughout the tax administration. • **Justification:** Data management activities should be transparent to different stakeholders. • **Implication:** Provide clear and accurate evidence of data management activities, controls used, data treatment, definitions, models and processes.	**Principle 4: Management control and audits.** • **Statement:** Data management (and governance) should be susceptible to audit and control. • **Justification:** Decisions, processes and controls related to data management should be auditable and document evidence to support compliance. • **Implication:** Formalize processes and operating models, ensuring evidence of compliance.
Principle 5: Accountability and data management • **Statement:** To govern data, the tax administration should define the boundaries of responsibility of the actors in data management and governance. • **Justification:** For data governance, it is essential to keep the responsibilities and management model clear and precise. • **Implication:** Adjust management processes, appropriate organizational structures to properly manage data, and integrate management practices in the tax administration.	

Source: CIAT (2022)

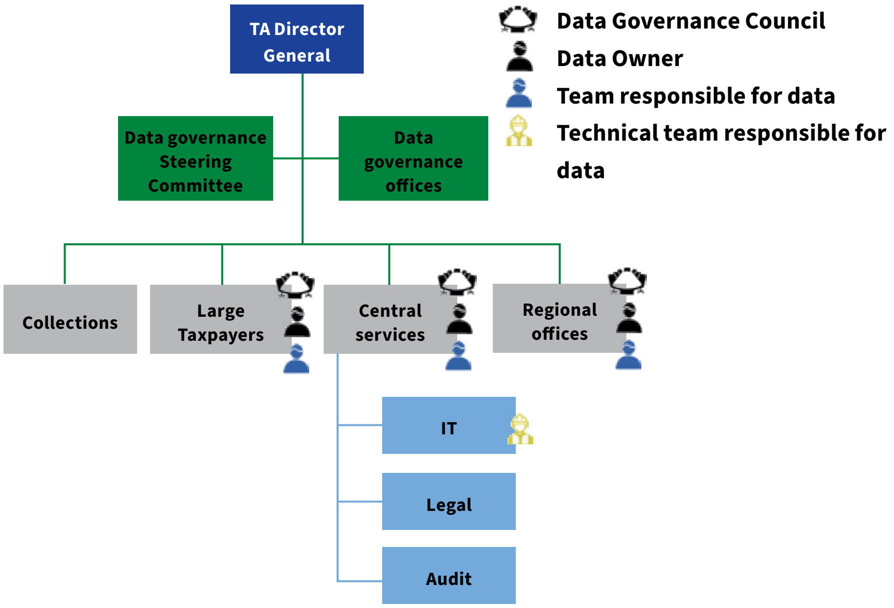
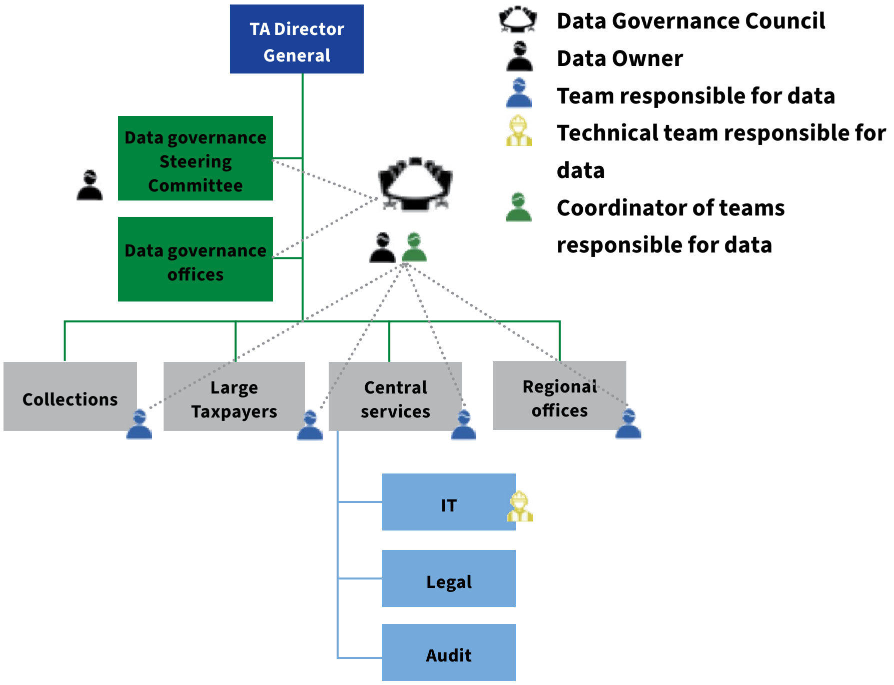
b) **Capabilities:** Sets out the core competencies that a tax administration should develop to ensure an effective data governance practice. When a TA adopts data governance for the first time, it is advisable to focus on developing core capabilities, e.g., defining the scope and alignment of the data strategy within the tax administration, as well as ensuring a commitment to the strategy at the management level. Once these capabilities are established, intermediate capabilities can be incorporated, for example, metadata management, risk management and data quality control, among others. Finally, advanced capabilities, such as data valuation management, can be considered. Although these are recommendations, the administration can adjust their development according to its particular needs.

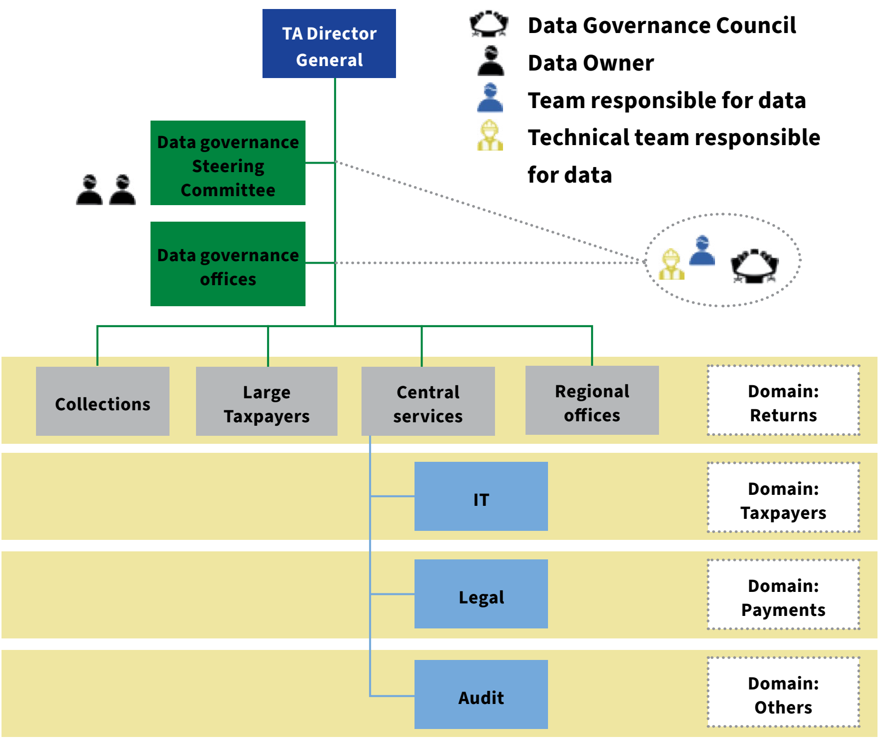
c) **Organizational structure, roles and responsibilities:** Depending on the TA's needs and available human resources, a structure is recommended to optimize data management within the entity, ensuring sound strategic direction and effective compliance with data governance policies. For example:

Data Governance Steering Committee	This is the main body within the tax administration. Formed by high-level executives responsible for data-intensive processes, such as the director of data or data governance manager, and the data owners/handlers. This committee has the primary responsibility of defining strategies, approving budgets, and prioritizing strategic decisions related to data management. Additionally, it collaborates with other high-level bodies and resolves organizational issues related to data.
Data Governance Council	This body is responsible for data management and governance activities, as well as handling data-related issues or incidents. It is formed by the Data Governance Manager, Data Stewards, and Data Architects. The council collaborates with various stakeholders to define and address data issues, resolve initial conflicts, and manage potential improvements throughout the tax administration's data lifecycle. It also ensures the effective implementation of data management and governance policies in coordination with the Data Governance Office, aligning efforts with the data strategy and tax objectives.
Data Governance Office	This unit is responsible for leading the definitions, control, and data management standards in the tax administration, promoting documentation, communication, and compliance with data policies. In small tax administrations where an independent unit is not feasible, it is recommended to share this function outside of the IT structure. The main responsibilities of the Office include documenting, supporting, publishing, and leading the activities and decisions of the Steering Committee and the Data Governance Council.

Source: CIAT (2022)

d) **Data governance organization:** It is essential to assess how to integrate data governance into the organizational structure of a tax administration to articulate and assign responsibilities. CIAT proposes three main models (i) functional, (ii) by type of taxpayer (e.g., large taxpayers, small and medium-sized enterprises, individuals, etc.), and (iii) a mixed model combining both approaches. Regardless of the model chosen, it is crucial to establish sound data policies and ensure coordination between Data Owners and Data Custodians in various departments, possibly with the support of Intermediate Data Governance Councils.

 TA Director General Data governance Steering Committee Data governance offices Collections Large Taxpayers Central services Regional offices IT Legal Audit Data Governance Council Data Owner Team responsible for data Technical team responsible for data	In large tax administrations, it can be beneficial to establish coordination between the Data Governance Councils and the Data Governance Office. Designating a single Data Owner can help to efficiently manage data shared among multiple stakeholders. Technical Data Administrators (the technical team responsible for the data) are centralized in IT. Furthermore, regulatory compliance is becoming increasingly important, requiring specific agents in business areas of tax institutions.
 TA Director General Data governance Steering Committee Data governance offices Collections Large Taxpayers Central services Regional offices IT Legal Audit Data Governance Council Data Owner Team responsible for data Technical team responsible for data Coordinator of teams responsible for data	In tax administrations, it can be useful to have three key entities: the Data Governance Steering Committee, the Data Governance Council, and the Data Governance Office. The Council centralizes tactical efforts by bringing together data owners and managers to address governance needs, while the Office coordinates operational executions and actively participates in the sessions of the Steering Committee and the Council through its designated leader.



In other tax administrations, an approach based on the specific data domains of the tax administration is an option. Data Administrators of each domain participate in the data governance council (for example, the Data Administrator for Large Taxpayers). Technical Data Administrators may also participate if necessary according to the organization or the data administrators.

Source: CIAT (2022) and CIAT (2024)

e) **Lightweight governance model:** When a tax administration aims to gradually incorporate data governance, it is often impractical to change its organizational structure. A lightweight approach could distribute responsibilities among existing units or collegial bodies. For example, control and compliance could be handled by the internal control unit, technological definitions could be handled by the IT department, while data quality would be handled by the data governance council, and strategy by the strategic committee. This not only optimizes resources but also fosters a culture of data management and improves data literacy throughout the organization. Although provisional, this model requires a data governance council at a minimum, which can start as a project team. It is recommended to eventually evolve into a more robust data management structure, starting with the formalization of a Data Governance Office.

f) **Data management:** Management includes mainly data managers from the functional area and technical data managers from the IT side. It is responsible for handling data responsibly, consistently and reliably. The following roles are recommended:

Data Managers	Responsibilities
Data Governance Officer	• Design and propose the data strategy to the Data Governance Steering Committee for approval. • Define and oversee data governance programs. • Appoint members of the Data Governance Steering Committee and the Data Governance Council. • Lead and coordinate decisions of both bodies. • Facilitate the identification and fulfillment of data needs. • Drive continuous improvements in the data governance model. • Integrate the governance model with other management models. • Develop and communicate data governance products. • Promote data governance practices within and outside the organization.
Data owner	• Approve data attribute/element definitions. • Define data quality dimensions and acceptable thresholds. • Ensure data quality and data definitions in your domain. • Lead necessary data changes. • Oversee data remediation and correction actions. • Authorize access and submission of data in accordance with security and privacy policies. • Responsible for data shared with other institutions. • Actively participate in the Data Governance Council as needed by the Steering Committee.
Functional data manager	• Execute or coordinate action plans to improve data quality. • Coordinate efforts to identify and address causes of data quality issues. • Support the Data Owner in definitions related to data in their domain, such as authoritative sources and quality rules. • Collaborate in defining data classifications and concepts within their domain.
Data custodian or technical data manager	• Support functional data managers with information, with data extraction, transformation and loading (ETL), and business intelligence (BI), etc. • Execute or support data quality improvements and data sources. This role, generally located in IT areas

Source: CIAT (2022)

g) **Data quality dimensions:** The dimensions allow to monitor and improve quality by establishing minimum tolerance thresholds. The selection of these dimensions should be based on the characteristics that best represent the current situation of the tax administration, in order to identify its priorities. The following is a summary of the different dimensions adopted in data quality:

Quality dimension	Definition
Accuracy	The degree to which the data represents the true value of the desired attribute in a specific context. For example, whether the registered address of a contributor is accurate.
Completeness	The degree to which the associated data has value for all defined attributes. For example, whether all tax obligations of taxpayers were completed.
Consistency	The degree of consistency with other existing data, eliminating inconsistencies. For example, a closed company or a deceased person should not file tax returns.
Integrity	The degree of accuracy and consistency of data. Ensures that the data is accurate and complete. For example, whether a legal representative identified by a taxpayer is registered.
Reasonableness	The degree to which the data is logical and conforms to reasonable expectations.
Timeliness	The degree to which data is updated and available within the required timeframe for its use. For example, real-time arrival of electronic invoice data to the tax administration.
Uniqueness	The degree to which data is not unnecessarily duplicated. For example, ensure that no entity exists more than once in the data set, ensuring that each unique entity has a unique critical value within the set.
Validity	The degree to which the data complies with the rules and definitions established for a specific purpose. For example, this includes expected data types, formats and precision, valid within a specific timeframe, such as uniform representation of dates.

Source: CIAT (2022) and DAMA

Although this list is not comprehensive, it can serve as an initial guide for developing a data quality strategy. However, it is recommended that each tax administration assess its main data quality issues and establish priorities to address them.

8.2. Generation of Quality Data

In recent years, organizations such as the OECD, the World Bank, the Inter-American Development Bank (IDB) and CIAT have developed tools and manuals specifically designed to strengthen tax administrations. These tools are aimed at facilitating significant improvement in terms of technology, modernization and adoption of international best practices. One of these instruments are the maturity models, widely used in self-assessment processes to measure current capabilities in specific functional, strategic or organizational areas. These models establish different maturity levels and criteria with the objective of providing a common vision of the necessary changes that an organization must implement to reach higher levels of development in the future, if it so chooses.

In 2022, the OECD published the Analytics Maturity Model, which encompasses two fundamental perspectives: strategic and operational. From the strategic perspective, the following attributes are evaluated:

a) **Strategy for analytical capabilities:** assesses whether the tax administration has an overarching strategy that covers the entire administration and whether it was formulated with the collaboration of external stakeholders.

b) **Governance**: analyzes whether the TA has a data governance board with external members to ensure harmonization between the administration's analytical processes and those used by other government entities and taxpayers.

c) **Culture**: measures whether the administration has an organizational culture that fosters innovation and continuous training, in which all levels of the organization understand and seek opportunities to apply data analytics, thus ensuring the optimization of the tax system.

d) **Budget**: examines whether the budget planning process for investment and expenditure in analytics is fully integrated into the budgeting processes of the entire administration.

The second perspective, operational, focuses on analyzing how management and management personnel support the development of the strategy and governance framework. Specifically, it focuses on assessing the following attributes:

a) **Technological (IT infrastructure)**: assesses whether a comprehensive IT infrastructure is in place for analytical services, including the existence of a centralized repository for data exploration in most systems.

b) **Data management**: assesses how data is managed over time, from collection to analysis and use.

c) **Talent management**: analyzes how human capital is managed and developed, using a structured approach to measure the effectiveness and evolution of talent management practices.

d) **Feedback**: measures the ability of TAs to use data and the results of their analysis effectively to continuously improve their processes and decisions.

e) **Project management**: examines the ability of TAs to effectively plan, execute and control data analytics initiatives. This includes the ability to clearly define project objectives, allocate adequate resources, and establish detailed plans to guide execution.

f) **Analytical capabilities**: assesses the TA's abilities to effectively collect, process, interpret, and use data to make informed decisions.

g) **Areas of use**: analyzes the extent to which data analysis is integrated into decision making.

Each perspective and attribute are assessed through the following five maturity levels:

a) **Emerging:** This level describes tax administrations that have begun to make progress in analytics, but still have a long way to go. At this stage, the achievements are emphasized and possible limitations are recognized.

b) **Progressing:** Here are tax administrations that have implemented or are implementing analytics reforms to approach the average level of advanced administrations.

c) **Established**: This level is typically achieved by advanced tax administrations, such as members of the Tax Administration Forum.

d) **Leading:** This represents the most advanced level currently possible through the tax administration's own actions.

e) **Aspirational:** This level considers what could be achieved in the medium term, as new technologies are adopted and progress is made towards a more efficient tax administration. It is recognized that achieving this level uniformly may be difficult due to the need for cooperation with external actors and other global challenges

Following the OECD model (2022), the table below details the indicative attributes and their means of verification according to the level of maturity in quality data generation and analytical capabilities:

Attribute	Means of Verification
Digitization	● **Emerging**: a significant number of data sources have not been digitized and digitized sources are maintained in independent systems. ● **Progressing:** most sources are digitized, and some data are centralized. ● **Established:** all major sources are digitized and there is a central repository for most data. ● **Leading:** there is access to a wide range of sources and unstructured data. ● **Aspirational:** there is a comprehensive repository shared with other agencies with near real-time access to third-party data.

Attribute	Means of Verification
Ontology and Metadata[62]	● **Emerging:** a common ontology and processes for creating and maintaining metadata are lacking. ● **Progressing:** there is awareness of the need for a common ontology, but it is not regularly implemented and while there is an attempt to create metadata it is inconsistent. ● **Established:** a common ontology is implemented and there are established processes for creating and maintaining metadata. ● **Leading:** there is advanced automation in ontology and metadata maintenance and integration with advanced analytical tools. ● **Aspirational:** there is full automation in ontology maintenance and rule translation and full integration with analytical tools.
Data Quality	● **Emerging**: little awareness of the importance of data quality, and limited documentation, with frequent errors and missing values. ● **Progressing**: some parts of the organization understand the importance of data quality and there is partially automated quality control. ● **Established**: there is widespread understanding of the importance of data quality, there are automated controls, and error correction exercises are conducted, although mostly manual. ● **Leading**: highly automated quality control and error correction. ● **Aspirational**: fully automated real-time quality control and error correction.
Talent Management	● **Emerging**: analyst training is provided through mentoring and self-study and there is a lack of structured development programs. ● **Progressing**: analyst career plans are unclear, making it difficult to retain talent, and minimal facilitation of training and promotion of competency development. ● **Established**: analyst selection through specific process, increasing prioritization of analytical competencies in selection processes, and there is organization of professional networks of analysts for skills exchange. ● **Leading**: defined career plans, establishment of links with universities with clear understanding of competencies needed, and structured support and training that encourages self-directed learning in advanced technologies. ● **Aspirational**: opportunities are offered up to managerial levels, there is close collaboration with universities for the design of career plans in the public sector and ongoing provision of professional courses and apprenticeships in various fields.

[62] **Ontology** refers to a comprehensive view of the common concepts, terms, and structures (metadata) used in tax administration. For example, in this area, both officials and IT systems should adopt a single definition of "taxpayer", thus establishing the corresponding ontology**. Metadata** refers to additional data that describes essential characteristics of the data elements. These can cover structural details such as the type of data and the number of records; quality aspects including validation rules, data quality, and information density; as well as relational aspects that indicate possible integration with data from other systems.

Attribute	Means of Verification
Feedback	● **Emerging**: there is sporadic evaluation of the results of data analysis, user feedback is collected informally and circumstantially, and learning is not systematically documented or applied in future projects. ● **Progressing**: evaluation of results is given at the end of projects, although not systematically and formal user feedback is given, although not always applied in future projects. ● **Established**: users test and review results during data analysis development, feedback is considered essential and applied to improve future projects, and lessons learned are formally documented and used for future improvements. ● **Leading**: results are evaluated according to predefined protocols and on a regular basis, there is comprehensive and structured quantitative and qualitative feedback on each project, results are systematically used to improve future projects, and there is external peer review. ● **Aspirational**: artificial intelligence is used to separate effects of analytics from other factors, there is continuous real-time monitoring of analytical models, and recommendations are incorporated according to continuous monitoring.
Project Management	● **Emerging**: analytical projects managed independently according to individual analysts' capabilities, with few formal processes. ● **Progressing:** some projects involve operational users, although involvement is intermittent due to limited resources. ● **Established:** operational users are reactively involved in analytical projects. ● **Leading:** operational users are fully integrated into advanced analytical projects, contributing ideas and ensuring that the results meet specific operational needs. ● **Aspirational**: multidisciplinary teams of operational users, project management experts, and analysts work together. Rigorous processes encompass advanced analytical applications such as artificial intelligence and real-time deployment, periodically validated and benchmarked against leading external organizations.
Analytical Capacities	● **Emerging**: data analysis based on limited assumptions, which may lead to incorrect conclusions. Analysts have basic skills in data management and visualization, but lack advanced statistical methodologies. ● **Progressing:** combines hypothesis-driven analysis, data exploration, and basic modeling, allowing discovery of unknown patterns. Advanced analysts possess modeling skills and understanding of the tax system. ● **Established:** focuses on data exploration and modeling with varied statistical techniques. Analysts perform systematic accuracy testing and use cross-validation methods. They have good command of statistical reasoning and strong capabilities in data management and visualization. ● **Leading:** uses structured and unstructured data, big data and advanced statistical techniques such as machine learning and artificial intelligence. Advanced analysts are skilled in statistical reasoning, various modeling techniques and data visualization. ● **Aspirational:** implements a complete set of tools for data visualization, natural language processing and machine learning. All analysts have a deep understanding of advanced techniques and statistical applications to solve complex operational problems.

Attribute	Means of Verification
Fields of Use	● **Emerging**: Limitations in the use of analytics and partial adaptation to the changing tax administration environment. ● **Progressing:** some departments use data analysts to combine data sources and support the fulfillment of tax duties, such as assessing risk profiles and uncovering serious anomalies. ● **Established:** use of sophisticated data analytics to detect anomalies, risks and potential issues related to tax legislation, with increasing automation to identify issues requiring further investigation. ● **Leading**: integration of analytics into a wide range of processes within tax administration, increasingly supported by artificial intelligence applications to identify issues and recommend automated or manual actions. ● **Aspirational:** data analytics is fully integrated into taxpayers' natural systems, simplifying compliance and reducing costs for both tax administration and taxpayers.

Source: OCDE (2022)

Investing in data quality is key for entities to fulfill their mission effectively and efficiently. While many of the more technologically advanced tax administrations recognize the importance of having high quality data, especially in the context of Big Data; few of the less technologically developed ones have taken concrete steps to ensure the quality of the data they receive.

Challenges and implications following the low quality of information:

1. Data duplication: *It is a common problem in tax administrations due to the lack of standardization in data formats. To mitigate this, it is essential to use specialized tools for data duplication. These solutions have evolved significantly and now have the capability to detect even notably different entries belonging to the same taxpayer.*

2. Inconsistent formats: *Systems face difficulties when there is a variety of data formats, such as in dates, tax identification numbers, and addresses. To address this challenge, it is crucial to establish clear guidelines for information entry and support them with validation rules that ensure data consistency.*

3. Incomplete information: *It is a significant problem for analytical tools and algorithms when data is entered in an incomplete, vague, or inconsistent manner. Implementing validation rules is an effective solution to ensure that records are not generated unless all essential information is included.*

4. Multiple units and languages: *They are a significant challenge, especially when there are differences in units of measurement and the management of special characters. It is essential to start by defining as* *many fields as possible as encoded identifiers. For example, instead of allowing text fields for entering descriptions, it is preferable to use previously defined catalogs. In this way, management can focus on developing data dictionaries that facilitate the improvement of analysis and information management.*

5. Inaccurate data: *There is a risk of using incorrect data in analyses and risk assessments. These issues are often difficult to detect, especially if the format is technically acceptable. For example, entering a valid but incorrect tax identification number. It is crucial for management to follow clear procedures and establish validation rules to improve the quality of information and ensure regulatory compliance.*

Source: *WB and CIAT (2022)*

8.3. International Scope

A review of OECD countries shows that countries such as Australia, Canada, the United Kingdom, among others have made significant progress in implementing legal frameworks and data governance strategies at the national level. These frameworks are designed to ensure that the management of their data across government meets rigorous standards of security, quality and efficiency. In tax administrations in these countries, digitization has become a central focus, leveraging advanced technologies to improve tax data collection and analysis. This approach not only facilitates taxpayer compliance but also strengthens management and oversight by tax authorities.

Lessons from South Korea – Digitalization Process

The digitization process in South Korea went through two distinct stages. From 1967 to 1996, the Tax Administration focused on automating processes and digitizing existing data through the installation of computers and training personnel. Although these efforts initially concentrated on data accumulation and building basic capabilities, as opposed to sophisticated data management or analysis, they laid the foundation for later developments.

Since the late 1990s, digitization has intensified on two main fronts. First, the government established an integrated infrastructure of databases to collect, store, and analyze tax data. This included the digitization of public services related to taxes, such as national identification, business registration, issuance of tax certificates, and online document submission, in addition to public-private collaborations for electronic invoicing systems, among others. Second, the implementation of laws and regulations to detect untraceable transactions and expose hidden income, modernizing data exchange between *institutions and clarifying benefits and penalties. In this way, unique schemes and incentives were designed to improve tax compliance in South Korea.*

In 2015, the tax administration introduced the New Integrated Tax System (NITSI), marking a significant advancement from the previous Integrated Tax System (ITS). The NITS unified more than 30 fragmented tax systems into a single cohesive system. This development was driven by the need to simplify data management, reduce administrative costs, and improve efficiency. The NITS consists of two main parts: the Next Generation National Electronic Tax System (NGH), designed as an online portal for taxpayers, and an internal portal for the Tax Administration that facilitates the operation of the NITS.

Source: *BID (2024)*

Australian Taxation Office (ATO)

During 2019 to 2022, the ATO experienced a significant 16% increase in debt accounts and a 70% increase in collectible debt due to the difficult economic conditions generated by the COVID-19 pandemic. After pausing many actions during the health crisis, in 2022 the ATO resumed its collection activities, implementing substantial improvements in its analytical capacity. In particularly:

1. The ATO improved its analytical models known as Financial Resilience Insights (FRI), allowing a more precise segmentation of its clients and a more accurate identification of their assets and income. In addition, it introduced Corporate Client Profiling (CCP) devices to gain a better understanding of the financial capacity of its taxpayers. This initiative allowed taxpayers with strong financial capacity to opt to pay in full or access shorter and more optimal payment plans, while those with less financial capacity were supported through longer and more sustainable payment plans, according to the analyses conducted.

2. The ATO adjusted the mix of analytical models to improve prediction accuracy and refocused on models that showed deterioration in performance due to lack of training data during the pause in the strongest collection actions.

3. In addition, the ATO evaluated the collection prospects for several specific groups of debtors, seeking to optimize recovery strategies according to the characteristics and risks of each group.

This detailed focus on the application of data science and analytical modeling reflects how the ATO responded to the economic challenges arising from the pandemic, using advanced tools to adapt its debt management strategies and improve the efficiency of its operations.

Source: *ATO*

Improvements in data integrity and quality in Sweden

Sweden has taken several measures to improve the quality of data related to tax administration:

1. GDPR compliance: The Swedish Tax Agency (Skatteverket) has implemented the European Union's data protection regulations (GDPR) in its personal data processing processes. This includes informing taxpayers about their rights and how their data is processed.

2. Special provisions for the Tax Agency: Sweden has established additional rules regulating what data the Tax Agency may process, for what purposes and for how long the data may be stored. This provides a robust legal framework for handling sensitive data.

3. Controlled information exchange: The Tax Agency shares information with other government agencies in a controlled manner and limited to what is strictly necessary for tax purposes, respecting the principles of proportionality and data minimization.

4. Use of data analytics: The Tax Agency is increasingly using data analytics tools to detect patterns and improve the identification and matching of taxpayer data.

Source: *Skatteverket*

9. Using the Cloud

The use of the cloud has played an important role in the digital transformation of tax administrations by improving the capacity to receive, store and process large volumes of data. As defined by the IDB (2020) [63] cloud computing encompasses more than just information storage. It is the delivery of on-demand services by technology providers and is done over the Internet or private networks.

Cloud computing services work in a similar way to a traditional IT environment, their difference lies mainly in how technological resources are managed, maintained and accessed. Cloud services are generally classified into three groups[64]:

- **Infrastructure as a Service (IaaS):** Cloud service providers offer consumers the opportunity to rent servers, storage, networks and other critical IT infrastructure resources. While the Service Provider manages and controls the infrastructure, the consumer has control over operating systems and storage. For example, virtual machines, cloud storage, virtual private networks and others are offered.

- **Platform as a Service (PaaS):** Cloud service providers allow consumers to deploy their own or purchased applications on the cloud infrastructure using tools provided by the provider. While the provider is responsible for managing and controlling the infrastructure, the customer retains control over the deployed applications. For example, *AWS Lambda, Azure App Service and low-code*[65] platforms among others.

- **Software as a Service (SaaS):** Service providers provide consumers with access to software applications running on cloud infrastructure. These applications can be used from different client devices via interfaces such as web browsers or program interfaces. The cloud provider handles most aspects of the SaaS

[63] Text available at: https://publications.iadb.org/es/publications/spanish/viewer/Computacion-en-la-nube-Contribucion-al-desarrollo-de-ecosistemas-digitales-en-paises-del-Cono-Sur.pdf

[64] Text available at: https://publications.iadb.org/en/publications/english/viewer/Cloud-Computing-Opportunities-and-Challenges-for-Sustainable-Economic-Development-in-Latin-America-and-the-Caribbean.pdf

[65] They provide a low-code development solution, which allows users to quickly create enterprise applications using a graphical interface without the need for extensive coding. The most well-known platforms include *OutSystems, Mendix, Appian,* among others.

offering, except for user-specific configurations for the applications. For example, Microsoft 365, Google *Workspace, ServiceNow* and others.

These services can in turn be presented under four deployment models, which depend largely on the consumer's requirements and uses.

- **Public cloud**: cloud designed to be open for public use. Users, whether individuals, academic institutions or companies, can contract the service to manage and operate the cloud, but the infrastructure exists on the provider's premises.
- **Private cloud**: cloud designed for the exclusive use of a single organization or entity, which provides greater control and security. Generally, this cloud can be hosted on-site at the organization's facilities (on-premise) or managed by an external provider, but it belongs exclusively to that organization.
- **Community cloud**: the cloud is designed for the exclusive use of a community or several organizations with a common interest; only the members of this community own, manage and operate the cloud.
- **Hybrid cloud**: combines two or more of the above infrastructures allowing interoperability between them. It can also integrate computing center services or on-premise infrastructure.

Currently, there are different providers of public cloud services offering a wide range of products and services that cater to various infrastructure, development, and software needs. For example, *Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), IBM Cloud, Oracle Cloud* among others. Each of these providers offers key services in computing, storage, databases, networking, and development tools. This allows consumers to build, deploy, and manage the necessary applications in the cloud with specific characteristics according to their needs. Additionally, these servers also allow the creation of virtual private networks within the public cloud, providing an isolated network environment.

9.1. Cloud Security

As mentioned earlier in the information security section, international standards in cybersecurity consist of a series of best practices, guidelines, and technical requirements aimed at ensuring the protection of information in organizations and systems globally. Their main objective is to facilitate the adoption and implementation of robust security measures, safeguard confidential data, manage risks, and ensure compliance with regulations in various jurisdictions around the world. In addition to ISO/IEC-27001, there are also standards for cloud security, specifically:

- **ISO-27017 Standard** – It establishes a series of recommendations and security practices relevant to the cloud services environment, helping organizations to more effectively manage the risks associated with this type of technology and to protect their information assets in a constantly evolving environment. The standard aims to improve information security in the cloud by implementing specific controls and practices, promoting greater trust and security for both providers and customers of cloud services.
- **ISO-27018 Standard** – provides a framework for the protection of personal data in public cloud services, to ensure that cloud service providers appropriately manage and protect their clients' personal information. This helps improve trust in cloud services and meet the privacy expectations and requirements of users and regulators. In this way, it seeks to ensure that personal data in the cloud is protected and managed according to best practices and applicable regulations, promoting greater security and privacy in the use of cloud services.

Additionally, there are System and Organization Controls (SOC)[66] reports, assessments conducted by independent external parties that demonstrate how a cloud service provider meets key compliance controls and objectives. These reports include information about internal controls related to financial reporting, as well as system security, availability, and security features and confidentiality compliance documentation. The security policy should require providers to submit documentation confirming that their services comply with third-party security certifications.

9.2. Benefits and Challenges of the Cloud

Although the adoption of cloud services has simplified access to digital technologies and provided governments with benefits such as reduced operational costs and increased efficiency in the delivery of public services, it also presents challenges that must be managed. The transition to the cloud, while offering opportunities for modernization and optimization, also poses risks related to data security, privacy, and dependence on external providers. Below are the main benefits and risks summarized, identified from the experiences of the countries of Central America, Panama, and the Dominican Republic.

[66] Read further in the following link: https://publications.iadb.org/es/publications/spanish/viewer/ Contratacion-publica-de-servicios-de-computacion-en-la-nube-Mejores-prácticas-para-su-implementacion-en America-Latina-y-el-Caribe.pdf

The substantial benefits of cloud adoption are summarized as follows:

- **Cost savings**: the cloud avoids large initial investments in physical infrastructure. Instead, a pay-as-you-go model is adopted that adjusts expenses according to the actual consumption of cloud resources. This approach not only reduces long-term operational and maintenance costs but also allows for adjusting spending according to the changing needs of the entity.

- **Scalability and flexibility**: the cloud allows governments to dynamically and agilely adapt their IT resources to respond to changes in demand without the need for additional investments in physical infrastructure. This scalability ensures that resources are available according to specific needs, whether during peak demand times or periods of lower activity, thereby optimizing performance and operational efficiency.

- **Access to emerging technologies and advanced tools**: the cloud facilitates access to emerging technologies and advanced tools, promoting continuous innovation. This enables governments to optimize operational efficiency and improve service quality.

- **Enhanced security**: cloud service providers offer access to a wide range of experts and cybersecurity tools, ensuring robust protection for information. Cloud infrastructure is equipped with advanced security measures, including encryption, continuous monitoring, and access controls, among others.

Some of the main challenges for the government's migration to the cloud are:

- **Legal restrictions**: in some countries the regulation does not allow data from the central administration or critical state information to be transferred to other jurisdictions. That is to say, the information must be hosted on national territory, preventing it from being managed by cloud service providers.

- **Budgetary restrictions:** in some countries, the use of open or multi-year contracts, involving variable payments, as happens with pay-per-use or on-demand cloud service models can be challenging. These regulations often classify spending on technology as an investment, leaving few options to treat these expenses as part of the current budget.

- **Required infrastructure for cloud services**: for the effective use of cloud services, countries need high-speed broadband networks, a reliable and constant power supply among others. These elements are essential for cloud service providers to offer their services efficiently and reliably.

- **Lack of knowledge and internal capabilities**: many government agencies lack the necessary knowledge about how cloud services operate and the required capabilities to manage virtual infrastructure, restructure processes, adapt to non-proprietary solutions, and manage outsourcing contracts.

- **Security, protection and privacy of data:** although service providers generally guarantee greater security in the cloud, the protection and privacy of data is a shared responsibility between data controllers (also known as users) and data processors. Data controllers must implement appropriate technical and organizational measures to protect personal data against illegal destruction, accidental loss, alteration, or unauthorized disclosure. Additionally, they must select processors that offer sufficient security measures. Cloud service users can use encryption to further protect their data, ensuring that only entities with the encryption keys can access the information.

9.3. Aspects to be Considered in Migrating Services to the Cloud

In 2023, the World Bank published a cloud assessment framework[67] that provides a list of key recommendations for entities responsible for acquiring these services. This framework offers valuable practices to consider for a safe and effective cloud adoption. In this section, the World Bank's methodology is referenced as a guide to assist countries in Central America, Panama, and the Dominican Republic in their migration processes. However, countries are encouraged to customize this checklist according to their specific contexts and particular needs.

- **Data classification:** according to the World Bank, data classification can be defined based on three security objectives commonly established in standards such as ISO 27001.
  - **Confidentiality,** means preserving authorized restrictions on access to and disclosure of information, protecting personal privacy and confidential information; a loss of confidentiality occurs with the unauthorized disclosure of information.
  - **Integrity,** means protecting information from unauthorized modifications or destruction, ensuring its authenticity; a loss of integrity manifests in unauthorized modification or destruction of data.
  - **Availability**, means ensuring timely and reliable access to and use of information; a loss of availability occurs when access to or use of information or an information system is disrupted.

Based on these objectives, it can be determined whether the data is public, official, secret, or top secret. This classification allows for determining the level of protection needed for each type of data and ensures that appropriate security measures are applied according to the sensitivity of the data. Public data, which has low sensitivity, requires less protection than confidential data or data requiring maximum confidentiality, which need stricter security measures due to their high level of sensitivity.

[67] The publication is available at the following link https://openknowledge.worldbank.org/server/api/core/bitstreams/60a6b421-da41-4c7c-9362-9ff277709281/content

	Public	Official	Secret	Top Secret
Impact on confidentiality, integrity and availability	**Low impact:** The loss of confidentiality, integrity or availability could be expected to have a limited adverse effect on organizational operations, organizational assets or individuals.	**Moderate impact:** The loss of confidentiality, integrity or availability could be expected to have a serious adverse effect on organizational operations, organizational assets or individuals.	**High Impact:** Loss of confidentiality, integrity or availability of data could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets or individuals.	**High Impact:** The loss of confidentiality, integrity or availability of **highly confidential** data could be expected to have an exceptionally serious adverse effect on organizational operations, organizational assets or individual**s.**

Source: World Bank (2022)

- **Data hosting:** according to the data classification level mentioned above, legal and security considerations must also be taken into account when deciding whether government data should be stored within the geographical boundaries of the country. Key considerations include analyzing whether other countries have adequate data protection laws and whether there are data transfer agreements with those countries. Additionally, it is important to consider the political stability and legal capacity of the countries where the data will be stored. To select suitable cloud providers, the following security requirements are recommended:

Security Requirements	Public	Official	Secret/ Top Secret
Certifications	No requirement (although alignment with certifications is recommended, example.g. ISO)	Certification required (e.g. ISO)	Certification required (e.g. ISO)
Data Location	Not required	The institution must determine whether an official data residency requirement should be established within the geographic boundaries of the country.	It is recommended that cloud service providers be required to ensure that data remains within the geographical boundaries of the country.
Type of cloud deployment	Public cloud	Public cloud	Private or community cloud (processing and storage is recommended to be on-premise).
Security clearance for service vendors	Not required	Not required	Required

Source: World Bank (2022)

- **Risk assessment and preparation:** it is recommended to consider conducting (i) an internal risk assessment to identify and analyze the risks associated with the integration of cloud services in the agency's current environment and (ii) a cloud readiness assessment to examine the agency's technical and operational capacity to effectively integrate and manage the cloud service. Conducting these assessments in advance ensures that the entity can not only handle the cloud service securely and efficiently but also meets the necessary technical and operational requirements for successful implementation.

- **Business case:** the preparation of a detailed business case is recommended for the adoption of the cloud service that includes the following elements:
  - Scope of the cloud service required.
  - Budget and calculation of the total cost of ownership.
  - Required skills of the personnel supporting the cloud services environment.
  - Infrastructure required to enable cloud service.
  - Expected benefits of the cloud service.
  - Outcome of the Risk and Preparedness Assessments.

- **Cloud security requirements**: the necessary security requirements for the cloud service contract must be identified and defined, based on the data classification levels of the relevant information systems.

- **Compliance with laws, regulations, and agency guidelines**: data security must comply with applicable national laws and regulations, as well as existing information security policies.

- **Contract**: a legally valid contract must be formalized with the cloud service provider before using the service.

- **Contract duration**: short-term contracts (two years or less) are recommended, with portability options to avoid excessive dependence on a single provider.

- **Data backup**: an effective data backup mechanism in the cloud must be coordinated with the cloud service provider.

- **Data protection and ownership**: it must be ensured that the cloud service provider does not claim ownership rights over the stored data, regardless of the format or storage medium. Additionally, an appropriate protection mechanism should be implemented.

- **Service continuity**: it should be ensured that the cloud service provider implements adequate cloud security controls and conducts regular tests of continuity and disaster recovery plans, communicating the results to the agency.

- **Continuous monitoring**: it is necessary to collaborate with the provider to maintain a secure environment in the public cloud. Activities may include security incident notifications and notifications of changes in security controls.

- **Data and application protection:** it must be ensured that, upon the termination of the service contract, all data and applications are transferred to a new service provider, returned to the agency, or permanently deleted, thus guaranteeing the protection and proper disposal of the information.

Guatemala Case:

In 2019, the Superintendencia de Administración Tributaria (SAT) of Guatemala became the pioneer institution in the use of the cloud in the country. Currently, SAT has two cloud platforms: AWS for transactional systems, such as the tax registry and electronic invoicing, and Azure for analytical functions, including the data warehouse. The decision to adopt cloud technologies was motivated by the need to efficiently manage electronic invoicing, which involves around 2 billion documents per year.

Benefits obtained by SAT by migrating services to the cloud:

- *Scalability and agility, by incorporating new government solutions quickly and efficiently.*
- *Modernization of tax administration*
- *Creation of operational efficiencies*
- *Increased storage and processing capacity*

Challenges and considerations when starting the migration process:

- *Ensure regulatory compliance*
- *Need for staff trained in new technologies*
- *Understanding how the cost/price of using the cloud works.*

Source: *SAT and AWS (2019)*

United Kingdom case:

G-Cloud is a UK government initiative designed to simplify the procurement of cloud services by government departments and encourage the adoption of cloud computing across government. The program consists of a series of framework agreements with cloud service providers, and an online store -the Digital Marketplace-, where these services are listed. This allows public sector organizations to compare and purchase services without the need for an extensive review process.

To be included in the Digital Marketplace, suppliers must self-assess and then undergo verification by the Government Digital Service (GDS), which acts at its discretion. In 2014, the G-Cloud onboarding process was simplified to reduce the time and cost to the UK government.

Rather than a centralized assessment of cloud services, the new process requires cloud service providers to self-certify and submit evidence in support of G-Cloud's 14 cloud security principles.

Source: *Microsoft (2024)*

References

Inter-American Development Bank. (2022). *Cloud Computing: Opportunities and Challenges for Sustainable Economic Development in Latin America and the Caribbean.* https://publications.iadb.org/en/publications/english/viewer/Cloud-Computing-Opportunities-and-Challenges-for-Sustainable-Economic-Development-in-Latin-America-and-the-Caribbean.pdf

Inter-American Development Bank. (n.d.). *Computación en la nube: Contribución al desarrollo de ecosistemas digitales en países del Cono Sur.* https://publications.iadb.org/es/publications/spanish/viewer/Computacion-en-la-nube-Contribucion-al-desarrollo-de-ecosistemas-digitales-en-paises-del-Cono-Sur.pdf

Inter-American Development Bank. (n.d.). *Contratación pública de servicios de computación en la nube: Mejores prácticas para su implementación en América Latina y el Caribe*. https://publications.iadb.org/es/contratacion-publica-de-servicios-de-computacion-en-la-nube-mejores-practicas-para-su

World Bank. (2022). *Data Classification Matrix and Cloud Assessment Framework: Cloud Assessment Framework and Evaluation Methodology.* https://openknowledge.worldbank.org/server/api/core/bitstreams/60a6b421-da41-4c7c-9362-9ff277709281/content.

Global Data Barometer. (2022). *Open Data Barometer y Data for Development.* https://opendatabarometer.org/leadersedition/report/

Canada Revenue Agency. (n.d.). *Taxpayer Bill of Rights*. https://www.canada.ca/en/revenue-agency/corporate/about-canada-revenue-agency-cra/taxpayer-bill-rights.html

CIAT. (2020). *Las TIC como herramienta estratégica para potenciar la eficiencia de las administraciones tributarias*. https://www.ciat.org/Biblioteca/Estudios/2020_TIC-CIAT-FBMG.pdf

CIAT. (2024). *Gobierno de datos para las administraciones tributarias.* https://biblioteca.ciat.org/opac/book/5884?_gl=1*1jdmgnn*_ga*MTk2NzA5MDM5NS4xNzIzMDg4MTI5*_ga_MHWYD6C0X9*MTcyOTA5NTEwMS41LjAuMTcyOTA5NTEwMS42MC4wLjA.

Costa Rica. *Sistema Costarricense de Información Jurídica.* (n.d.). http://www.pgrweb.go.cr/scij/avanzada_pgr.aspx

Declaration of the Rights of Humans and Citizens. https://www.conseil-constitutionnel.fr/sites/default/files/as/root/bank_mm/espagnol/es_ddhc.pdf

El Salvador. Ministerio de Hacienda. (n.d.). https://www.mh.gob.sv/

El Salvador. Portal de Transparencia Fiscal. (n.d.). https://www.transparenciafiscal.gob.sv/ptf/es/MarcoNormativo/AdministracinTributaria.html

United States. Internal Revenue Service. (n.d.). https://www.irs.gov/

Góngora Pimentel, G.D. (n.d). *Estudios en Homenaje a Héctor Fix Zamudio – El reconocimiento del Derecho Administrativo Sancionador en la Jurisprudencia Constitucional Mexicana*, IIJ – UNAM, México.

Guatemala. Superintendencia de Administración Tributaria. (n.d.). https://portal.sat.gob.gt/portal/

HM Revenue & Customs, *The HMRC Charter,* Reino Unido. Información disponible en https://www.gov.uk/government/publications/hmrc-charter/the-hmrc-charter

Honduras. Servicio de Administración de Rentas. (n.d.). https://www.sar.gob.hn/

Huerta, C. (n.d.). *Sobre la distinción entre derechos fundamentales.* Corte Interamericana de Derechos Humanos. https://www.corteidh.or.cr/tablas/r28772.pdf

Internal Revenue Service. (n.d.). *Carta de Derechos del Contribuyente – versión en español.* Documento disponible en: https://www.irs.gov/es/taxpayer-bill-of-rights

KPMG. (2019). *The role of internal audit in cyber security readiness*. https://assets.kpmg.com/content/dam/kpmg/lu/pdf/2019/lu-en-cyber-databreach-brochure.pdf

Mexico. Servicio de Administración Tributaria (n.d.). https://www.sat.gob.mx/home

National Institute of Standards and Technology. (n.d.). https://www.nccoe.nist.gov/data-security

Organization of American States (OAS). (n.d.). *Convención Americana sobre Derechos Humanos – Pacto de San José.* https://www.oas.org/dil/esp/1969_Convenci%C3%B3n_Americana_sobre_Derechos_Humanos.pdf

Organization of American States (OAS). (2013). *El Acceso a la Información Pública, un Derecho para ejercer otros Derechos*. https://www.oas.org/es/sap/dgpe/concursoinformate/docs/cortosp8.pdf

Organization of American States (OAS). (2021). *Principios Actualizados sobre la Privacidad y la Protección de Datos Personales*. https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf

United Nations. (n.d.). *Declaración Universal de los Derechos Humanos – Resolución 217A (III).* https://www.ohchr.org/sites/default/files/UDHR/Documents/UDHR_Translations/spn.pdf

United Nations. (n.d.). *Derechos Humanos.* https://www.un.org/en/global-issues/human-rights

OECD. (2017). *Estándar para el Intercambio Automático de Información sobre Cuentas Financieras.* https://www.oecd.org/es/publications/estandar-para-el-intercambio-automatico-de-informacion-sobre-cuentas-financieras-segunda-edicion_9789264268074-es.html

OECD. (2021)., *Guía Práctica sobre Confidencialidad y Gestión de la Seguridad de la Información.* https://web-archive.oecd.org/tax/transparency/documents/confidentiality-ism-toolkit_es.pdf

OECD. (2020). *Panorama de las Administraciones Públicas América Latina y el Caribe 2020.* https://doi.org/10.1787/1256b68d-es

OECD. (2024). *Panorama de las Administraciones Públicas: América Latina y el Caribe 2024.* https://doi.org/10.1787/0f191dcb-es.

OECD. (2007). *Perspectivas de la OCDE. Capital Humano: Cómo moldea tu vida lo que sabes. Resumen en español.* https://www.oecd-ilibrary.org/docserver/9789264029095-sum-es.pdf?expires=1721158015&id=id&accname=guest&checksum=0B33A3E116BBA88CA0AA16B137FEB6E9

OECD. (n.d.). *Recomendación del Consejo de la OCDE sobre el Gobierno Abierto.* https://www.oecd.org/gov/oecd-recommendation-of-the-council-on-open-government-es.pdf

OECD. (2020). *Response of Tax Administrations to COVID-19: Considerations about the continuity of activities and services defines essential activities as those functions in which time is a critical factor whose unavailability or malfunction, even for hours, would affect the administration's business continuity systems, people, buildings and suppliers, leading to an unacceptable level of disorganization in their work and interruption of their activities, deterioration of customer service or reputational damage.* https://read.oecd-ilibrary.org/view/?ref=133_133006-nruwv5tdpl&title=Respuesta-de-las-administraciones-tributarias-al-COVID-19-Consideraciones-acerca-de-la-continuidad-de-actividades-y-servicios

OECD. (n.d.). *Taxpayer's Rights and Obligations – Practice Note.* https://www.oecd.org/tax/administration/Taxpayers'_Rights_and_Obligations-Practice_Note.pdf

OECD. (2022). *Modelo de Madurez de Análisis de Datos.* https://www.oecd.org/content/dam/oecd/en/topics/policy-issues/tax-administration/modelo-de-madurez-de-analisis-de-datos.pdf

International Organization for Standardization. (n.d.). https://www.iso.org/es/home

Panama. Dirección General de Ingresos. Ministerio de Economía y Finanzas. (n.d.) https://dgi.mef.gob.pa/

Prodecon. (2014). *Transparencia, Secreto Fiscal y Uso Indebido de Comprobantes*. https://portal.prodecon.gob.mx/Documentos/analisis-sistemicos/estudios-tecnicos/secreto-fiscal/mobile/index.html#p=1

Dominican Republic. Dirección General de Impuestos Internos. (n.d.) https://dgii.gov.do/Paginas/default.aspx

Rüdiger, P. (1990). *Human Resource Management: An international comparison*. Human Resource Management: An International Comparison – Google Libros

Sebastian-Coleman, L. (2018). *Navigating the labyrinth: An executive guide to data management* (1st ed.). Technics Publications.

Servicio de Administración Tributaria de México. (n.d.). *Carta de los derechos del contribuyente auditado.* http://omawww.sat.gob.mx/informacion_fiscal/derechos_contribuyentes/Documents/Carta_Contr_Aud_072014.pdf

UNESCO. (n.d.). *Access to Information Laws.* https://www.unesco.org/en/access-information-laws

Annex

Legal framework on confidentiality, access to information and transparency

Country	Confidentiality of information			Access to Information and Transparency			Sanctioning Framework
	Political Constitution	Tax Code	Data Protection	Political Constitution	Access to Information Laws	Transparency Laws	Additional or Complementary Regulations
Costa Rica	Article 30	Code of Tax Rules and Procedures. Article 115, 115 bis and 117	Law on the Protection of the Individual Against the Processing of their Personal Data - Law N° 8968 Regulation of the Law on the Protection of the Person with regard to the Processing of their Personal Data N° 37554-JP,	N/A	Transparency and Access to Public Information N° 073-MP-MEIC-MC Executive Decree No. 40199-MP Opening of Public Data		N/A
El Salvador	N/A	Article 28	General Guidelines for the Protection of Personal Data	N/A	Law on Access to Public Information	N/A	Special Law against IT and Related Crimes
Guatemala	Article 24	Article 101-A	Comprehensive Law on the Protection of Personal Data Held by Third Parties *	Article 30 Article 31	Law on Access to Public Information	N/A	N/A
Honduras	Article 182	N/A	Personal Data Protection Law and Habeas Data Action	N/A	Law on Transparency and Access to Public Information		N/A
Panama	Article 29 Article 42	Article 722	Law 81 for Data Protection	Article 43 Article 44	Law on Transparency and Access to Information – Law 6 of January 22, 2002.		N/A
Dominican Republic	Article 44	Article 47	Law no. 172–13 Comprehensive Protection of Personal Data (…)	N/A	General Law on Free Access to Public Information No. 200–04.		

✉ ciat@ciat.org