



UNODC

United Nations Office on Drugs and Crime

A CLOSER LOOK:

A TOOLKIT FOR BENEFICIAL OWNERSHIP TRANSPARENCY AND
ENHANCED SCRUTINY OF POLITICALLY EXPOSED PERSONS

UNITED NATIONS OFFICE ON DRUGS AND CRIME

A CLOSER LOOK:

**A TOOLKIT FOR BENEFICIAL OWNERSHIP TRANSPARENCY AND
ENHANCED SCRUTINY OF POLITICALLY EXPOSED PERSONS**



UNITED NATIONS
Vienna, 2024

Disclaimers:

© 2024, United Nations Office on Drugs and Crime (UNODC)

Recommended citation: UNODC. 2024. A Closer Look: A Toolkit for Beneficial Ownership Transparency and Enhanced Scrutiny of Politically Exposed Persons.

The designations employed and the presentation of material in this paper do not imply the expression of any opinion whatsoever on the part of the United Nations Office on Drugs and Crime (UNODC) concerning the legal or development status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

Images: © istock/unsplash

Editing: Jaya Mohan

Graphic design and layout: Gerda Palmethofer

UNODC encourages the use, reproduction and dissemination of material in this information product. Except where otherwise indicated, material may be copied, downloaded and printed for private study, research and teaching purposes, or for use in non-commercial products or services, provided that appropriate acknowledgement of UNODC as the source and copyright holder is given and that UNODC's endorsement of users' views, products or services is not implied in any way.

This publication has not been formally edited.

ACKNOWLEDGEMENTS

This publication was developed by the United Nations Office on Drugs and Crime (UNODC), with the support of generous funding from the Foreign, Commonwealth and Development Office of the United Kingdom of Great Britain and Northern Ireland and the Bureau of International Narcotics and Law Enforcement Affairs of the United States of America.

The development of the publication is the result of the collective efforts of numerous individuals and organizations who share a commitment to understanding and combating the complex challenges of illicit financial flows, money laundering and terror financing through Beneficial Ownership Transparency (BOT) and the enhanced scrutiny of politically exposed persons.

UNODC, therefore acknowledges with profound gratitude all those who have contributed their expertise and experience to the development of this publication:

Mr. Gibson Chizanda (Zambia),
Ms. Leone Dunn (Namibia),
Mr. Andrea German (Botswana),
Ms. Adri Grobler (Banking Association of South Africa)
Adv. Xolisile Khanyile (South Africa),
Ms. Pleasure Matshego (South Africa),
Mr. Sebastiao Rocha (Angola). Ms. Sukai Tongogara (Zimbabwe)
Ms. Lize van Schoor (South Africa)

Special thanks to Ms. Carla Constantinescu for her support in liaising with the 8 country representatives and the Open Ownership team consisting of Ms. Karabo Rajuili, Mr. Timon Kiepe, Ms. Alanna Markle and Mr. Stephen Abbot Pugh for their review and insightful comments.

UNODC also wishes to thank the experts Ms. Katerina Nicolaou (Technical Adviser, Argent Econ Consult (Pty) Ltd) and Ms. Yuchen Wu (post doctorate student at Ludwig Maximilian University of Munich) for their substantive contribution to the drafting of this toolkit.

UNODC wishes to acknowledge the responsibility for the overall coordination, focus and substantive development of this publication ensured by Mr. Itumeleng Mongale, UNODC Africa Anti-Corruption Hub.

CONTENTS

<i>Acronyms</i>	7
<i>Glossary</i>	9
<i>Executive summary</i>	15
<i>Overview and introduction</i>	22
<i>A PEP and BOT toolkit</i>	36
Legislation and structure: decision framework	38
Strategy and action: policy framework	42
Systems, tools and technologies: technology framework	46
Processes: technical framework.....	83
Monitor, analyse and enforce: monitoring, evaluation and learning framework	89
Service, staff, skills and resources: resource framework	91
Communication and collaboration: stakeholder engagement framework.....	94
Bringing 7 pillars together	95
<i>Recommendations and conclusions</i>	98
<i>References</i>	104

ACRONYMS

AEOI	Automatic Exchange of Information
AI	Artificial Intelligence
AML/CFT	Anti-money laundering and countering the financing of terrorism
BODS	Beneficial Ownership Data Standard
BOT	Beneficial Ownership Transparency
CbC	Country by Country
CDD	Customer Due Diligence
CEO	Chief Executive Officer
CENFRI	Centre for Financial Regulation and Inclusion
CFO	Chief Financial Officer
CRS	Country Reporting Standard
COO	Chief Operating Officer
CSO	Civil Society Organization
DID	Decentralized Identifiers
DLT	Distributed ledger technologies
DNFBP	Designated Non-Financial Businesses and Professions
EDD or ECDD	Enhanced Due Diligence or Enhanced Customer Due Diligence
EIOR	Exchange of Information on Request
EITI	Extractive Industries Transparency Initiative
ESAAMLG	Eastern and Southern African Anti-Money Laundering Group
EU	European Union
FACT	Financial Accountability and Corporate Transparency
FATF	Financial Action Task Force
FDI	Foreign Direct Investment
FI	Financial Institutions
FIC	Financial Intelligence Centre
FICA	Financial Intelligence Centre Act
FIU	Financial Intelligence Unit
GDP	Gross Domestic Product
GIZ	The Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH
GFI	Global Financial Integrity
HIO	Head of International Organization
HLP	High Level Panel
IASB	International Accounting Standards Board
ICC	International Chamber of Commerce
ICIJ	International Consortium of Investigative Journalists
IDB	Inter-American Development Bank
IFF	Illicit Financial Flows

IFRS	International Financial Reporting Standards
IMF	International Monetary Fund
KYC	Know Your Customer
LEA	Law Enforcement Authorities
LEI	Legal Entity Identifier
LLC	Limited Liability Corporation / Company
MCAATM	Multilateral Convention on Administrative Assistance in Tax Matters
MERL	Monitoring, Evaluation, and Learning Framework
ML	Money laundering
MLA	Mutual Legal Assistance
MOU or MOA	Memorandum of Understanding/Agreement
NGO	Non-Government Organization
NPC/NPO	Non-Profit Company / Organization
NRA	National Risk Assessment
OECD	Organisation for Economic Co-operation and Development
OGP	Open Government Partnership
OSINT	Open-Source Intelligence
PBO	Public Benefit Organization
PCC	Protected Cell Companies
PEP	Politically Exposed Person
PIP	Prominent Influential Person
PSC	People with Significant Control
POC	Proceeds of Crime
POPI	Protection of Personal Information
RBA	Risk Based Approach
SARs/STRs	Suspicious activities or transactions
SOC	State-Owned Company / Corporation
SRB	Self-Regulating Body
SSA	Sub-Saharan Africa
SSI	Self-sovereign identity
StAR	Stolen Asset Recovery Programme (an initiative of the World Bank Group and the UNODC)
SWOT	Strengths, Weaknesses, Opportunities and Threats
TF	Terror/Terrorist Financing
TIEA	Tax Information Exchange Agreement
TIN	Trader Identification Number
UNCAC	United Nations Convention Against Corruption
URI	Uniform Resource Identifiers
UWOs	Unexplained Wealth Orders
VI	Verifiable Identifiers
VP	Vice President
VTDPs	Voluntary Tax Disclosure Programmes
WB	World Bank
WCO	World Customs Organization

GLOSSARY

Attribute: A named quality or characteristic inherent in or ascribed to someone or something.¹ In ID systems, common identity attributes include name, age, sex, place of birth, address, fingerprints, photo, signature, identity number, etc.

Authentication: The process of establishing confidence that a person is who they claim to be. Digital authentication generally involves a person electronically presenting one or more “factors” to “assert” their identity—that is, to prove that they are the same person to whom the identity or credential was originally issued. These factors can include something a person knows (e.g., a password or PIN), has (e.g., an ID card, token, or mobile SIM card), or is (e.g., their fingerprints).² There are different types of authentication usage, namely (a) “Two-factor” authentication, which involves more than one of the factors described above (i.e., two things that you are, know, or have).³

Authoritative source: An authoritative source of identity information is a repository or system that contains attributes about an individual and is considered to be the primary or most reliable source for this information. In the case that two or more systems have mismatched or have conflicting data, the data within the authoritative data source is considered the most accurate.⁴

Beneficial owner: In the context of legal persons, beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those natural persons who exercise ultimate effective control over a legal person (such as a company or arrangement such as a trust). Only a natural person can be an ultimate beneficial owner, and more than one natural person can be the ultimate BO of a given legal person.

Beneficial Ownership Data Standard (BODS): BODS is a framework for publishing structured data about beneficial ownership, developed by Open Data Services and Open Ownership in a format that can be read and understood by computer systems around the world. BODS has been adopted by both governments and the private sector, and a range of tools and applications have been developed around it. Refer to <https://standard.openownership.org> for more detail.

1 NIST. 2017. SP 800-63:2017 *Digital Identity Guidelines*. Available at <https://pages.nist.gov/800-63-3/>.

2 Ibid.

3 Although authentication and verification are related and often used interchangeably, for the purposes of this toolkit, they can be distinguished by whether the process involves determining the veracity of particular attributes (verification) or ensuring that a person is the “true” owner of an identity or credential (authentication). In some cases, however, authentication procedures go beyond establishing a legitimate claim to an identity and verify particular attributes. For BO, it means ensuring that the person making a statement about BO is who they say they are and involves verifying and validating the identity of individuals who hold significant interests in legal entities. It ensures that the disclosed beneficial owners are indeed the rightful holders of those interests by assuring that the documents and information provided are legitimate.

4 FICAM (n.d.). *Streamline Identity Management Playbook. United States Federal Identity, Credential, and Access Management*. Available at: https://bnbuckler.github.io/ficam-identity/2_step-2/.

Bearer Negotiable Instruments: Bearer Negotiable Instruments (BNIs) includes monetary instruments in bearer form such as: traveller's cheques; negotiable instruments (including cheques, promissory notes and money orders) that are either in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery; or, incomplete instruments (including cheques, promissory notes and money orders) signed, but with the payee's name omitted.

Big data: represents datasets whose size is beyond the ability of typical database software tools to capture, store, manage, and analyse. Big data has high volume, high velocity and high variety.⁵

Blockchain: A system in which a record of transactions made in bitcoin, or another cryptocurrency are maintained across several computers that are linked in a peer-to-peer (P2P) network. "Distributed ledger technologies (DLTs), like blockchain, enable multiple members to maintain their own identical copy of a shared ledger. Rather than requiring a central authority to update and communicate records to all participants, DLTs allow their members to securely verify, execute, and record their own transactions without relying on a middleman."⁶ DLTs have the following building blocks: (a) they are public or private ledgers; (b) they are permissioned / permission-less distributed ledgers; (c) they have a consensus algorithm (to ensure all copies of the ledger are identical); and (d) there is a framework that incentivizes or rewards participation for the 'work' undertaken.

Competent authority: Competent authorities as defined by the Financial Action Task Force (FATF) refers to all public authorities with designated responsibilities for combating money laundering and/or terrorist financing. In particular, this includes the Financial Intelligence Units/Centres (FIU/FIC); the authorities that have the function of investigating and/or prosecuting money laundering, associated predicate offences and terrorist financing, and seizing/freezing and confiscating criminal assets; authorities receiving reports on cross-border transportation of currency and BNIs; and authorities that have Anti-Money Laundering and Counter Terror Financing (AML/CFT) supervisory or monitoring responsibilities aimed at ensuring compliance by financial institutions and Designated Non-Financial Businesses and Professions (DNFBPs) with AML/CFT requirements. Self-Regulating Bodies (SRBs) are not to be regarded as a competent authority.

Credential: A document, object, or data structure that vouches for the identity of a person through some method of trust and authentication. Common types of identity credentials include – but are not limited to ID cards, certificates, numbers, passwords, or SIM cards. A biometric identifier can also be used as a credential once it has been registered with the identity provider⁷ (adapted from reports). Credential, in the digital identity world applies an identity "credential"

5 Laney (2001). Others have expanded on this definition adding other attributes (while keeping to the V theme), including variability, validity, value, and veracity, among others (NIST Big Data Public Working Group, 2015a, p. 7).

6 Hedera Hashgraph. (n.d.). *What are distributed ledger technologies?* | Hedera Hashgraph. [online] Available at: https://hedera.com/learning/what-are-distributed-ledger-technologies-dlts?gclid=CjwKCAiAkJKCBhAyEiwAKQBCKq4o3TUZz0AC7pvgeW2dt-og4oiw4zQjcQ_vj_9fUMne61-MjFby3BoCoTMQAvD_BwE, accessed 18 February 2021.

7 ID4D (2016). *Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation*, A joint World Bank Group–GSMA–Secure Identity Alliance Discussion Paper. Available at <http://documents.worldbank.org/curated/en/600821469220400272/Digital-identity-towards-shared-principles-for-public-and-private-sector-cooperation>

which is preferred to identity “document” in most contexts as many digital credentials are not physical documents.

Data ingestion engines (also called loaders or connectors): is the process of obtaining and importing data for immediate use or storage in a database in either real-time or in batches. The ‘engine’ is essentially the driver programme that integrates the data from various data sources, addressing the data interoperability issues.

Data lake or data pond: a system or repository of data stored in its natural/raw format, usually in files or object blobs (Binary Large Object stored as a single entity). A data lake is usually a single store of data including raw copies of source system data, sensor data, social data etc., and transformed data used for tasks such as reporting, visualisation, advanced analytics and machine learning. A data lake can include structured data from relational databases (rows and columns), semi-structured data (CSV, logs, XML, JSON), unstructured data (emails, documents, PDFs) and binary data (images, audio, video). Data lakes can be physical data centres or in the cloud.

Data swamp: is a deteriorated and unmanaged data lake that is either inaccessible to its intended users or is providing little value.

Data Trust: is a legal and technical framework designed for sharing and managing data. It aims to promote and facilitate data sharing among organizations while ensuring trust in the rules, data security, confidentiality, and privacy.⁸ A data trust is a legal structure that provides independent stewardship of data. It involves groups of people or organizations that collect and hold data, allowing an independent institution (the data trust) to make decisions about how that data is used and shared for an agreed purpose. The trustees of the data trust take on these responsibilities and associated liabilities.⁹

Digital identity: set of electronically captured and stored attributes and credentials that uniquely identify a person.¹⁰

Digital identification system: An identification system that uses digital technology throughout the identity lifecycle, including for data capture, validation, storage, and transfer; credential management; and identity verification and authentication.¹¹

Distributed ledger technology: see *Blockchain*.

Designated non-financial businesses and professions (DNFBPs): include casinos; real estate agents; dealers in precious metals and/or precious stones; lawyers, notaries, other independent

8 Creme Global (n.d.). *What is a Data Trust? The Complete Guide for organisations, regulators and manufacturers*. Available at [What is a Data Trust? The complete guide for organizations, regulators and manufacturers](#). - Creme Global

9 ITPRO (2020). *What are data trusts and how do they work?* Available at: <https://www.itpro.com/in-depth/354740/what-are-data-trusts-and-how-do-they-work>

10 Harbitz, M. and K. Kentala. (2013). *Dictionary for Civil Registration and Identification*. Washington, DC: Inter-American Development Bank. Available at: <https://publications.iadb.org/en/dictionary-civil-registration-and-identification>

11 Ibid., ID4D (2016).

legal professionals and accountants;¹² trust and company service providers refers to all persons or businesses that are not covered elsewhere under the FATF recommendations.

Financial institutions: Financial institutions means any natural or legal person who conducts as a business one or more of the following activities or operations for or on behalf of a customer: acceptance of deposits and other repayable funds from the public; lending; financial leasing; money or value transfer services; issuing and managing means of payment;¹³ financial guarantees and commitments; traders in money market instruments, foreign exchange, exchange, interest rate and index instruments, transferable securities, and commodity futures trading; participation in securities issues and the provision of financial services related to such issues; individual and collective portfolio management; safekeeping and administration of cash or liquid securities on behalf of other persons; and investing, administering or managing funds or money on behalf of other persons.

Legal arrangement: refers to express trusts and other similar legal arrangements. Examples of other similar arrangements (for AML/CFT purposes) may include but are not limited to *fiducie*, *treuhand* and *fideicomiso*.

Legal person: refers to any entities other than natural persons that can establish a permanent customer relationship with a financial institution or otherwise own property. This can include companies, bodies corporate, foundations, partnerships, or associations and other relevantly similar entities

Nominee shareholder or director: Nominee is an individual or legal person instructed by another individual or legal person (“the nominator”) to act on their behalf in a certain capacity regarding a legal person. A Nominee Director (also known as a “resident director”) is an individual or legal entity that routinely exercises the functions of the director in the company on behalf of and subject to the direct or indirect instructions of the nominator. A Nominee Director is never the beneficial owner of a legal person. A *Nominee Shareholder* exercises the associated voting rights according to the instructions of the nominator and/or receives dividends on behalf of the nominator. A nominee shareholder is never the beneficial owner of a legal person based on the shares it holds as a nominee.

Machine-readable data: Machine-readable data is structured data that can be understood and processed by computers without human intervention. It contrasts with human-readable data, which is designed primarily for human consumption. Machine-readable data can take various formats, including:

- CSV (Comma-Separated Values): A tabular format where data is organized into rows and columns.
- JSON (JavaScript object notation): A lightweight data interchange format commonly used for APIs and web services.

¹² this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to ‘internal’ professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to AML/CFT measures

¹³ For example, credit and debit cards, cheques, traveller’s cheques, money orders and bankers’ drafts, electronic money

- XML (Extensible markup language): Designed to be both human- and machine-readable, often used for data exchange.
- RDF (Resource description framework): A standard for representing information about resources on the web.
- Other structured formats: These formats ensure that data can be processed efficiently by software.

Machine-readable data enables automation, data analysis, and integration across systems. It allows computers to extract relevant information, perform calculations, and generate insights without manual effort. Remember, machine-readable data is not synonymous with digitally accessible data. While a document may be available online, true machine readability requires structured data that computers can process effectively.

Obligated entity: a professional subject to customer due diligence obligations when entering into business with a customer or carrying out a transaction, that is making the necessary verifications on the identity of their customer and the origins of the funds. Those include financial institutions and Designated Non-Financial Bodies and Professions (DNFBPs), as per FATF terminology.

Politically exposed persons: Foreign Politically Exposed Persons (PEPs) are individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials. Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials. Persons who are or have been entrusted with a prominent function by an international organization refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions. The definition of PEPs is not intended to cover middle ranking or more junior individuals in the foregoing categories

Red flags/red flagging: Red flags are a set of criteria that are consistent with suspicious companies or individuals and can be used to identify these in each Member's dataset. Red flagging is the process of raising red flags.

Trust: refer to legal arrangements.

Trustee: The terms trust and trustee should be understood as described in and consistent with Article 2 of the Hague Convention on the law applicable to trusts and their recognition. Trustees may be professional (e.g. depending on the jurisdiction, a lawyer or trust company) if they are paid to act as a trustee in the course of their business, or a non-professional who is not in the business of being a trustee (e.g. a person acting on behalf of family).

Trust and company service providers: all persons or businesses that provide certain services to third parties, such as: (i) acting as a formation agent of legal persons; (ii) acting as director or secretary of a company, a partner of a partnership or a similar position in relation to other legal persons; (iii) providing a registered office; business, correspondence or administrative address

for a company, a partnership or any other legal person or arrangement; (iv) acting as a trustee of an express trust or performing the equivalent function for another form of legal arrangement; (v) acting as a nominee shareholder for another person.

Shell Bank: Shell bank means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. Physical presence means meaningful mind and management located within a country. The existence simply of a local agent or low-level staff does not constitute physical presence.

Shell company: Shell companies are legal entities that are non-operational and lack assets or staff. While these corporate structures often have legitimate functions, they are also an attractive type of anonymously owned company for money launderers, who can use them in combination with other (often legal) techniques to keep their identity hidden from government authorities and to funnel funds across borders. Often, owners choose to hide their identity by incorporating their entities in different jurisdictions to make use of domestic legislation to hide their wealth from authorities and obfuscate the trail (to their identity and wealth, thereby evading taxes).

Self-sovereign identity: A form of decentralized digital identity created by an individual and remains under their control. By attaching trusted information (credentials) from authoritative sources to these identities, the individual can create trust in the claims he or she makes about his or her identity, while still maintaining that control. Blockchain technology, could be employed in a future decentralized identity framework, as well as how decentralized identity can be an enabler of important blockchain use cases.

Verification: see authentication.

EXECUTIVE SUMMARY

This toolkit aims at defining the necessary measures needed to eliminate or at the very least, hinder financial crime in countries by emphasizing the importance of identifying and scrutinizing Politically Exposed Persons (PEPs) and Beneficial Owners (BOs) that hide their ill-gotten wealth behind various layers or veils of corporate opacity. Financial crime links up with activities such as money laundering, terror financing, corruption and tax evasion. The basic premise is that PEPs, due to their position, are more exposed to corruption. The toolkit defines PEPs as individuals who are or have been entrusted with prominent public functions, including foreign PEPs, domestic PEPs, and those with roles in international organizations. These individuals are considered to have significant political influence and access to resources, presenting a higher risk for involvement in unlawful activities such as corruption, embezzlement and bribery. On the other hand, BOs are defined as natural persons who ultimately own or control a legal entity or arrangement, benefiting from its assets or conducting transactions on its behalf. This definition goes beyond legal ownership to include the exercise of direct or indirect control over an entity, aiming to unveil the actual individuals who benefit from or control transactions through legal entities and arrangements.

In order to expose the ultimate beneficiaries at the apex of legal entities or arrangements, financial and related information should be stored in centralized databases or registries that are able to communicate with other such platforms to share information seamlessly across jurisdictions. A key to creating such joined-up systems is to ensure that initiatives on BO and transparency are based upon internationally accepted mechanisms and frameworks like the Financial Action Task Force (FATF) recommendations so that the same sort of information is collected and classified in a similar manner. This information can then be used to mount appropriate law enforcement actions that can bring the guilty to book.

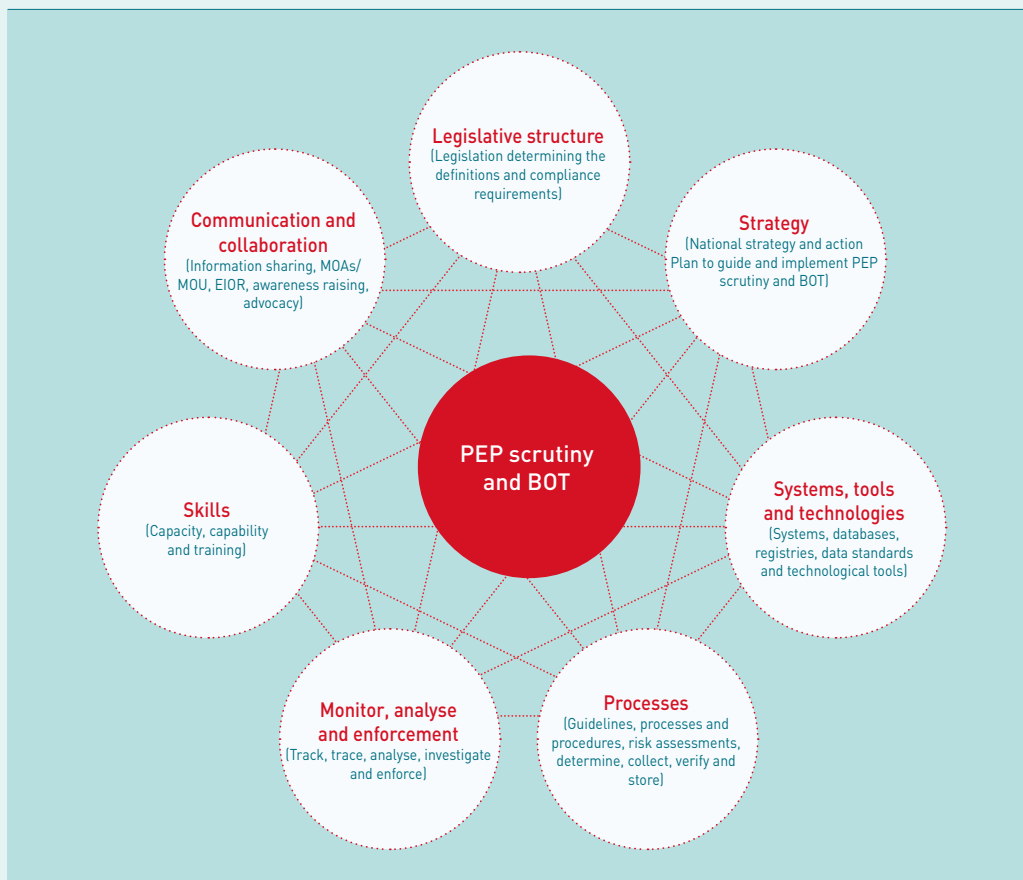
PEP and BOT toolkit

The toolkit rests on seven pillars highlighted in the figure below. Disclosure frameworks that use these principles have a much greater chance of BO data being used to deliver the desired policy impact on focused and specific uses cases including the combating of money laundering, terror financing, tax evasion and illicit financial flows at national and international levels.

The core elements of this guiding framework for an effective Beneficial Ownership Transparency (BOT) and PEP scrutiny, unites the following focal areas:

- reform of the legal framework;
- development of a national strategy, action plan and agenda;
- creation of technical systems and tools for analysis;
- development of the policies and procedures to collect, store, verify, update, analyse and share information;
- mechanisms to monitor, track and trace beneficial owners and scrutinize PEPs;
- highlight the skills, resources and capacity required; and
- the communication, publication of data and collaboration to share information within a country's institutions and across jurisdictions.

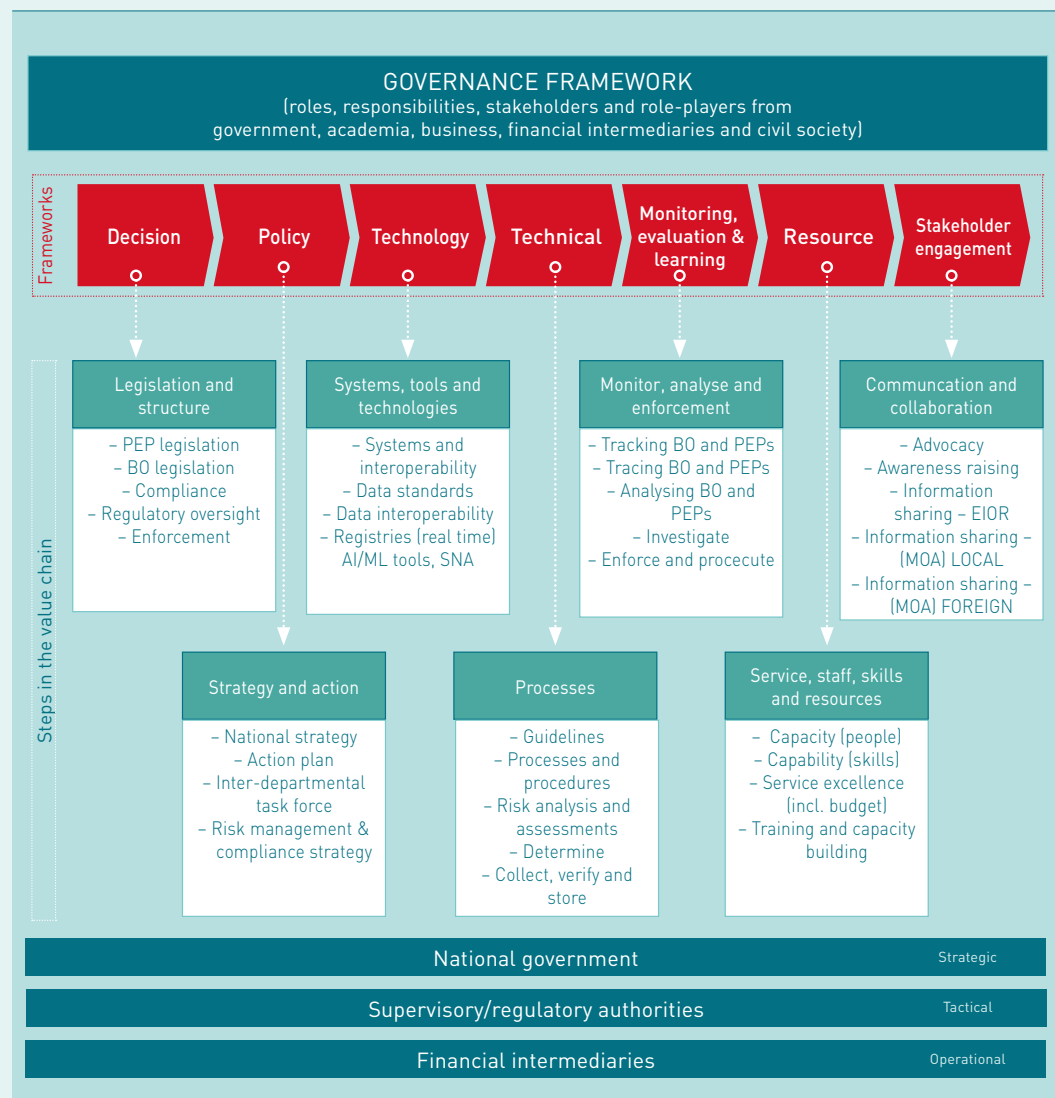
Figure 1: Pillars of an effective framework for PEP scrutiny and BOT



Although work on each area is often undertaken by different experts and departments, these seven components must work together in a synergistic manner for a holistic, integrated BOT and PEP scrutiny mechanism that effectively curbs money laundering, terror and proliferation financing, corruption, and tax evasion, ensuring that the data can be usefully applied across the board.

Figure 2 highlights the various steps in the value chain necessary to build a comprehensive, integrated BOT and PEP scrutiny mechanism.

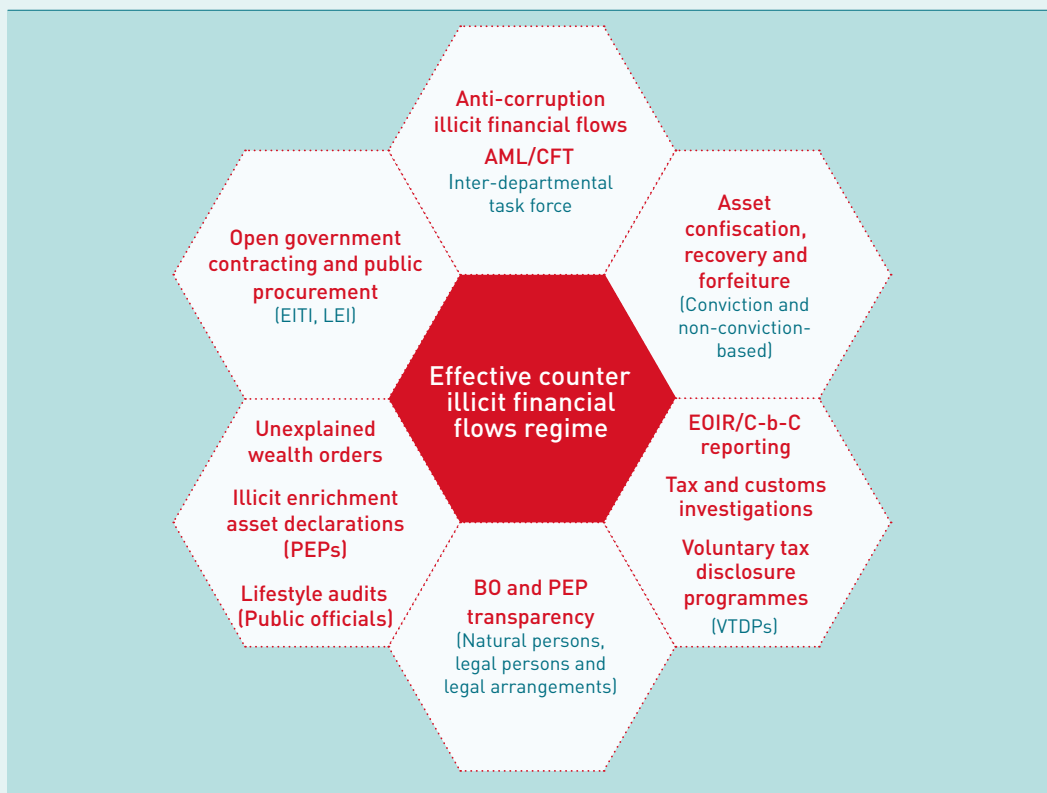
Figure 2: Components and stages necessary in the value chain to build a comprehensive, integrated BOT and PEP scrutiny mechanism



To begin with, a central BO registry, held by a public authority or body functioning as a BO registry should be developed. This centralization ensures efficient access to the information. However, countries can use an alternative mechanism that also enables rapid and efficient access to BO information. “This includes the multi-pronged approach, which consists of combining information from, among others, companies themselves, public authorities in a registry, or alternative mechanism if it ensures rapid and efficient access to BO information. FATF’s mutual evaluations demonstrated that countries using a multi-pronged approach were more effective in preventing the misuse of legal persons for criminal purposes and ensuring transparency of BO than countries using a single approach.”¹⁴

14 FATF (2023). *Guidance on Beneficial Ownership of Legal Persons*. Available at: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-Beneficial-Ownership-Legal-Persons.html>.

Figure 3: Technical components of the PEP and BOT toolkit



It is important that these databases are co-related so that a complete picture is available. The central BO registry should include PEP information and interface with the PEP register.

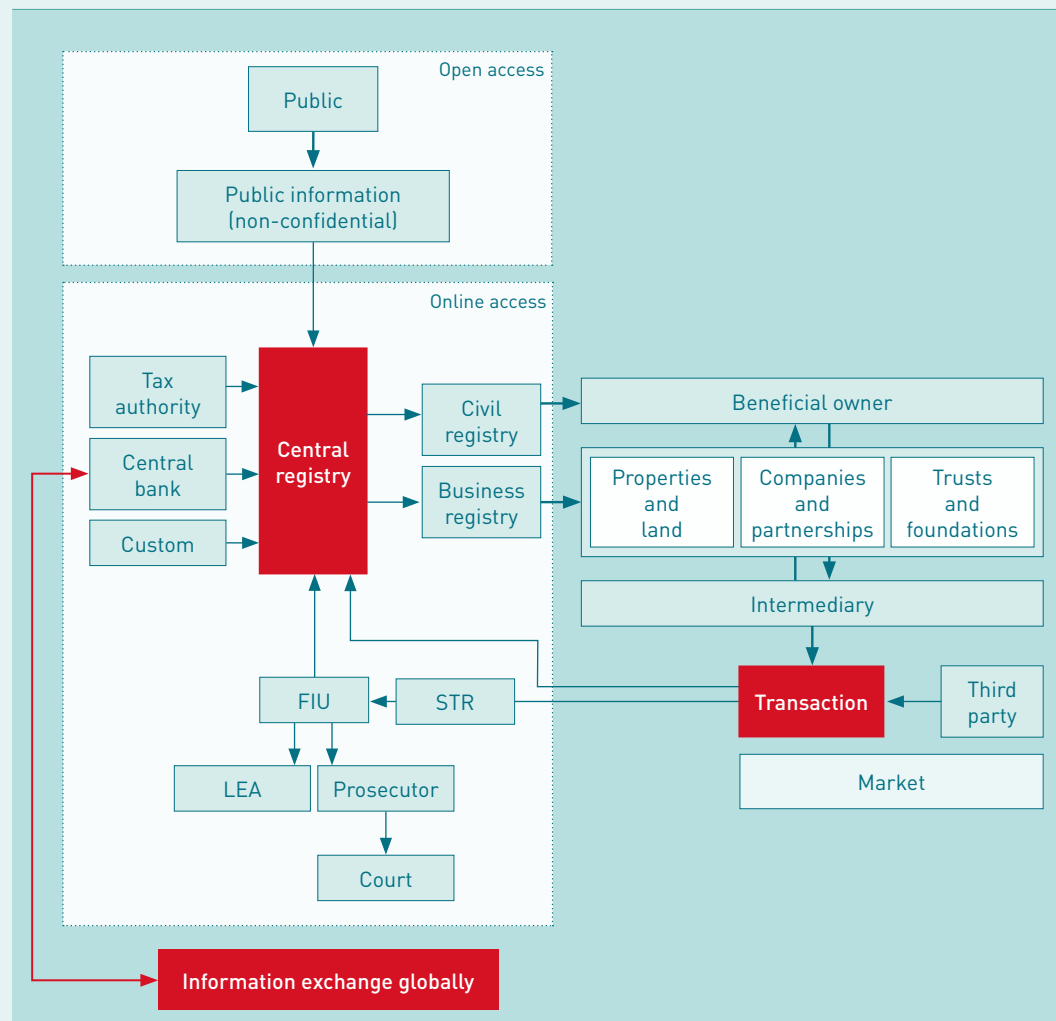
Similarly, the trusts register should include BO information and should also interface with the central ownership register.

To close the net, Financial Intelligence Units (FIUs) and Law Enforcement Authorities (LEAs), should stitch together a series of public and privately available data (including information submitted by financial institutions such Suspicious Transaction Reports or Suspicious Activity Reports) and analyse this inter-operable information linked to the central BO register to track, trace and analyse the information, evaluating suspicious transactions or red flagging them for further investigation to assess whether criminal activity has taken place, i.e., criminal activity, money laundering, terror financing, corruption and tax evasion. This information is passed on to the public prosecutor, who in turn prosecutes the perpetrator/s. Moreover, the tax and customs authorities as well as the central bank should have vetted and secure access to the information in the central registry.

Information in the central registry should ideally be accessible in real-time, and updated, verified and maintained on a regular basis. In March 2022, the FATF agreed on tougher global BO standards, where countries are now required to ensure that competent

authorities have access to adequate, accurate, and up-to-date information on the true owners of companies. It is imperative that there are data standards that ensure that the data is accessible by numerous government agencies (promoting data interoperability), by sharing the information with pre-approved government agencies and LEAs in other jurisdictions.

Figure 4: A central registry with numerous third-party data interfaces



Finally, the public could have access to certain credentials of the BO information in the central registry.¹⁵ Moreover, financial institutions, including Designated Non-Financial

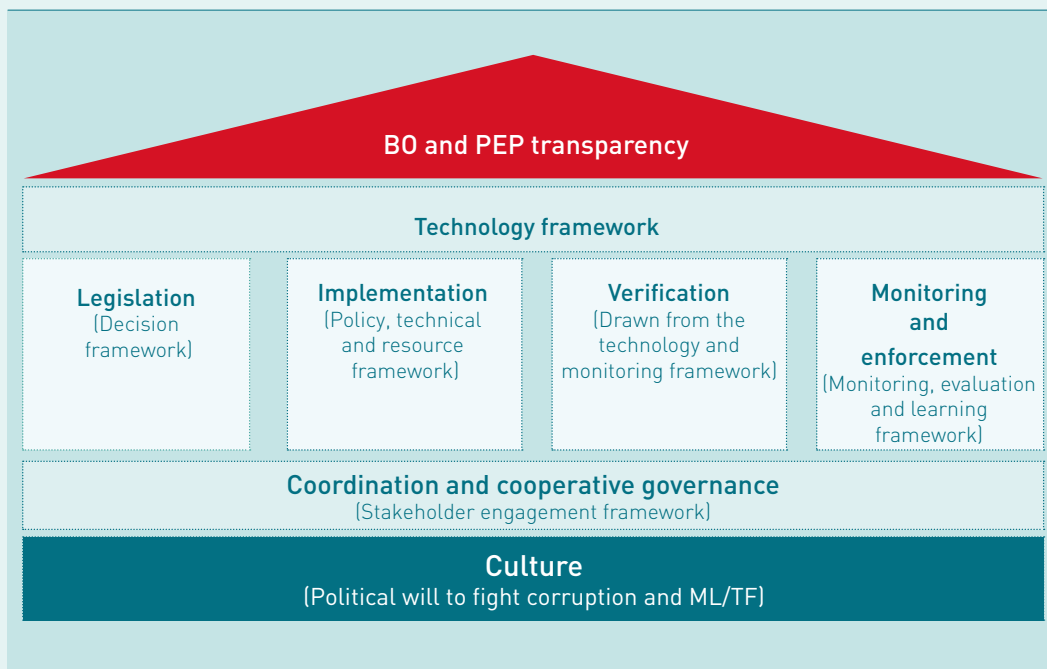
¹⁵ In its judgement of 22 November 2022, the Court of Justice of the European Union (the 'Court') invalidated the requirement introduced by the European Union Directive 2018/843 ('AMLD5') that Member States should make information on the BO of legal entities held in central registers accessible in all cases to any member of the public. The Court considered that such public access was neither strictly necessary to prevent ML and TF, nor proportionate and could therefore not justify a serious interference with fundamental rights, namely the right to respect for private life and to the protection of personal data enshrined in Articles 7 and 8 of the Charter. The latest FATF recommendations requires a central BO register to be held by a public authority, but it does not have to be a public register.

Businesses and Professions (DNFPBs) and other supervisory authorities should be allowed secure, yet controlled access to the central registry.¹⁶

It is recommended that countries have a multi-pronged central registry sourcing information from multiple public and private sources, while ensuring a combination of tiered, secure (and public) access, where law enforcement and similar authorities and other designated users have full authorized access to all the information in the register while the public could have access to discrete pieces of less sensitive information (ensuring that individual’s personal information is protected and that they are not exposed to various crimes including identity theft, stalking, kidnapping, etc.).

The seven frameworks fit together to create a holistic and effective BO and PEP transparency toolkit, which includes some suggestions relating to digital innovation.

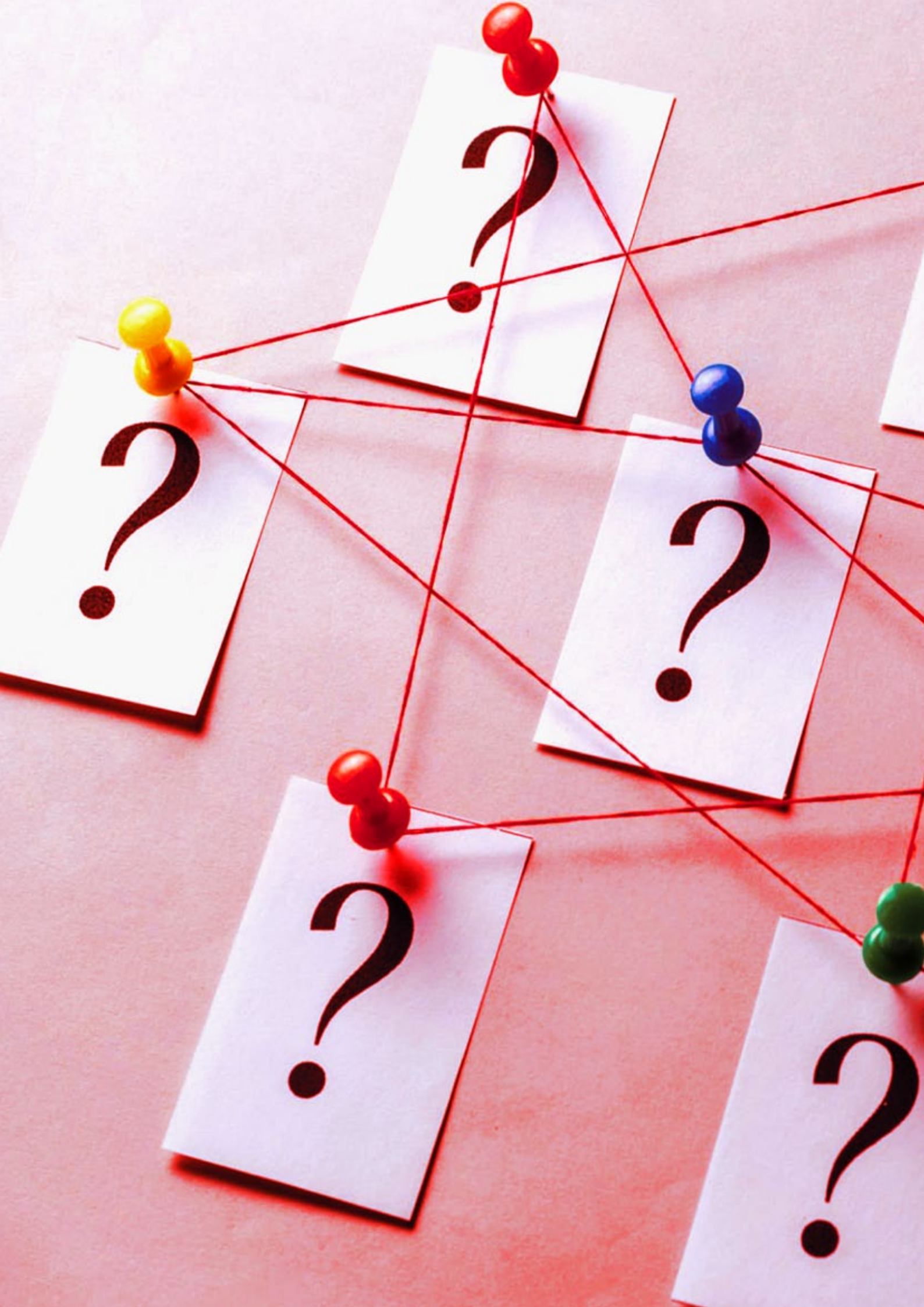
Figure 5: Seven areas of action to implement an effective BOT and PEP transparency framework



The end-to-end toolkit on the scrutiny of PEP and BO was originally developed in 2021. It has been updated according to the latest FATF recommendations. In 2021, the toolkit was beta tested in a handful of Southern African countries through a questionnaire evaluating the seven pillars or frameworks of the toolkit, assessing the ability of competent authorities to scrutinize PEPs and BO information in addressing money laundering, terror financing, corruption and tax evasion to mention a few. The seven pillars or frameworks were then converted into an easy and useful graphic addressing:

¹⁶ This registry should be available online, through webservice or other similar technologies.

- legislation, which represents the decision framework;
- technology, which refers to the technology framework;
- implementation, representing the policy, technical and resource frameworks;
- verification, an important component of the technology, process, monitoring, analysis and enforcement frameworks;
- monitoring and enforcement, referring to the monitoring, evaluation and learning framework;
- coordination and cooperative governance, aligning with the stakeholder engagement framework; and
- culture, relating to the political will to fight corruption, money laundering, terror financing, tax evasion and illicit financial flows.





*Overview and
introduction*

In the intricate fabric of modern global finance, the misuse of corporate vehicles remains a significant avenue for masking illicit activities. From money laundering to evading sanctions and concealing illicit gains, the exploitation of opaque ownership structures undermines the integrity of financial systems and fuels the engine of transnational crime worldwide.

Corporate vehicles/entities can be misused to circumvent controls by disguising the identity of known or suspected criminals and the source of their funds or assets. However, this misuse could be significantly reduced if accurate information regarding both the legal owner and the ultimate beneficial owner or the natural person, the source of the corporate vehicle's assets and its activities, were readily available and used by the authorities. It is often very difficult for concerned authorities to identify the natural, real person who truly has ownership and control of a company, trust or other corporate vehicle, particularly when the corporate structure involves several countries. By setting up one or more corporate vehicles, criminals are able to obfuscate their identity, and with it, the true purpose, source or use of funds or property associated with the corporate vehicle.

Similarly, by hiding behind the corporate veil of opacity, a Politically Exposed Person (PEP) can use their position of power and influence and abuse the trust of the public and the public institutions they oversee in order to benefit personally. Owing to their status and sway, numerous PEPs occupy roles that are susceptible to misuse for personal enrichment through corruption and bribery. While money laundering (ML) is often a subsequent act to conceal such ill-gotten gains rather than the primary intent of the abuse, it remains intricately linked with these predicate offenses. Additionally, such positions of power may also be exploited for activities associated with terrorist financing (TF). The potential risks associated with PEPs justify the application of additional anti-money laundering / counter-terrorist financing (AML/ CFT) preventive measures with respect to business relationships with PEPs.

The Financial Action Task Force (FATF) has issued detailed recommendations for country governments to implement to address ML, TF, corruption and bribery for self-enrichment by PEPs, and the criminals hiding behind corporate vehicles. In order to prevent this form of abuse, it recommends using a risk-based approach (RBA) which requires financial institutions and designated non-financial businesses and professions (DNFBPs) to implement a RBA that mitigates risks through the following measures that:

- prevent the misuse of the financial system and non-financial businesses and professions by PEPs through recommendations 12 and 22. These requirements are preventive (not criminal) in nature, and should not be interpreted as stigmatising PEPs as such being involved in criminal activity¹; and
- prevent legal persons or arrangements from being misused for criminal purposes, through recommendations 24 and 25, which include the following:

1 Refusing a business relationship with a PEP simply based on the determination that the client is a PEP is contrary to the letter and spirit of Recommendation 12.

- assessing the risks associated with legal persons and legal arrangements;
- making legal persons and legal arrangements sufficiently transparent; and
- ensuring that accurate and up-to-date basic and BO information is available to competent authorities in a timely fashion.

These FATF standards lay the groundwork that supports the efforts to prevent and detect other designated categories of offences such as tax crimes and corruption and asset accumulation by PEPs. In this respect, the measures that countries implement to enhance transparency in line with the FATF recommendations may provide an approach to more effectively address serious concerns such as corruption, as well as to meet other international standards.²

Financial transparency, in particular the transparency of BO of legal entities and arrangements (including those owned by PEPs), is a useful policy tool available to governments to address illicit financial flows (IFF), ML, TF, tax and trade crimes, bribery and corruption.

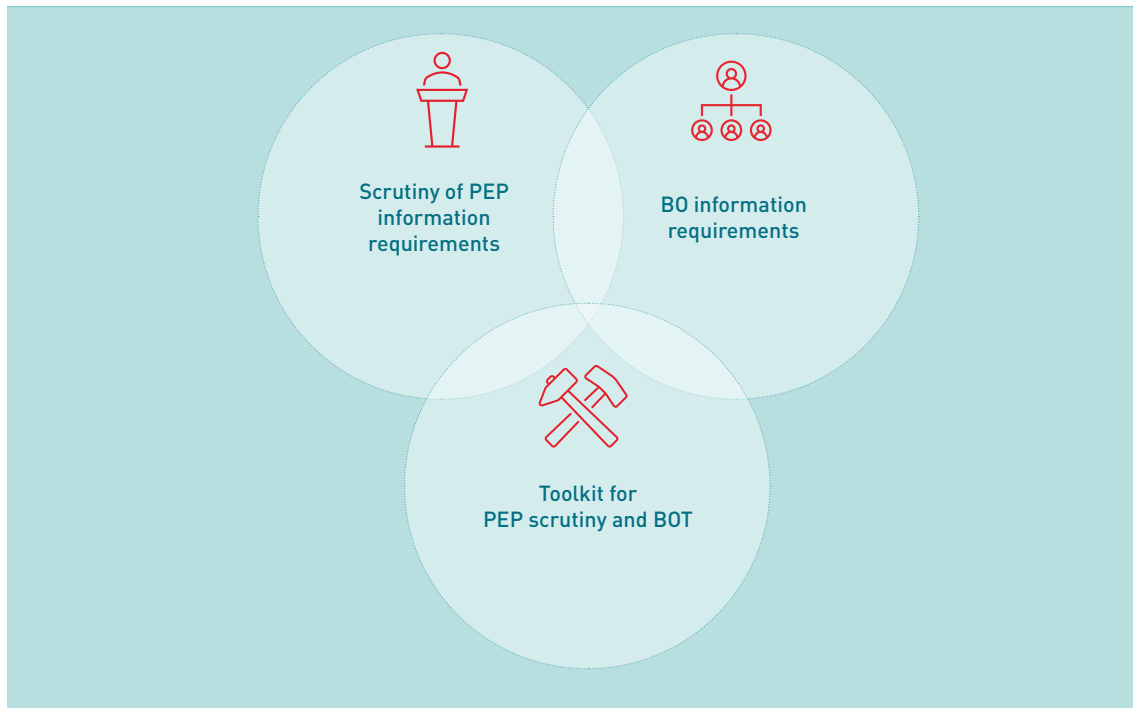
This toolkit is an essential stride towards unmasking the BO of corporate entities, a vital step in the global fight against corruption and financial crime.

Purpose of this publication

International standards require minimum levels of transparency concerning the scrutiny of PEPs and the beneficial owners of legal entities and arrangements for AML/CFT purposes. This toolkit develops an approach to address PEP scrutiny and beneficial ownership transparency (BOT) in the form of a handbook. The information is presented in a *visually appealing and simple manner*. It collates all the findings and produces a series of recommendations using a plug-and-play approach, based on best practices. However, this is framed by the capability and capacity to implement BOT and PEP scrutiny systems on each country. The toolkit is therefore presented in a *modular way for countries*, depending on the sophistication of their legislation and policies, their systems, and institutional and leadership appetite, allowing them to implement the systems in a stepwise or modular manner.

² Such as the United Nations Convention Against Corruption (UNCAC), the Criminal Law Convention on Corruption, and the OECD Convention on Combating the Bribery of Foreign Public Officials in International Business Transactions.

Figure 1: Overlaps between PEP scrutiny and BO information



Politically Exposed Persons and Beneficial Ownership Transparency

Politically Exposed Persons (PEPs)

The issue of PEPs is one of the most important points of intersection between AML/CFT and the anti-corruption agenda. Strengthening PEPs scrutiny can result in economic and developmental benefits for countries on the African continent. “Dealing with corrupt PEPs poses difficult challenges of ‘guarding the guardians’, as these individuals are by definition politically influential and generally command substantial resources.”³

Empirical evidence points to corruption having a negative effect on economies that far outweigh the positive effects.⁴ Corruption adversely affects economic performance, reduces the quality and quantity of public and private investment and contributes to lower tax revenues, a weakened financial system with “adverse distributional effects as it hurts the poor disproportionately. Countries with high levels of corruption achieve lower literacy rates, have higher mortality rates,

3 Sharman, J. (2009). [online] Regional Seminar on Political Economy of Corruption: Politically Exposed Persons (PEPs). Griffith University, Australia, 9 September 2009, ADB Headquarters, Manila, Philippines. ADB/OECD Anti-Corruption Initiative for Asia and the Pacific. [Oecd.org. Available at: https://www.oecd.org/site/adboecdanti-corruptioninitiative/meetingsandconferences/44442190.pdf](https://www.oecd.org/site/adboecdanti-corruptioninitiative/meetingsandconferences/44442190.pdf), accessed 8 January 2021.

4 FATF (2011). Laundering the Proceeds of Corruption. PDF. <https://www.fatf-gafi.org/media/fatf/documents/reports/Laundering%20the%20Proceeds%20of%20Corruption.pdf>, accessed 10 December 2020.

and overall have worse human development outcomes. Corruption deepens poverty by reducing pro-poor public expenditures, by creating artificial shortages and congestion in public services, and by inducing a policy bias in favour of capital intensity, which perpetuates unemployment.”⁵

The International Consortium of Investigative Journalists (ICIJ) identified a list of PEPs who were shareholders, directors and beneficiaries of offshore companies by studying the massive Panama Papers data leak on 10 May 2016. The disclosures implicated at least 140 politicians from more than 50 countries in tax evasion schemes.⁶ The owners of the anonymously-owned companies created by Panama-based law firm Mossack Fonseca had previously been kept secret due to the opaque nature of offshore jurisdictions. Ironically, some world leaders featured in the leaked documents from Mossack Fonseca had embraced anti-corruption platforms.

The FATF defines a PEP as “an individual who is or has been entrusted with a prominent function.” This definition is also used in article 52 of the United Nations Convention against Corruption (UNCAC).

The FATF defines a PEP as follows (FATF, 2023b):

- **Foreign PEPs** are individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.
- **Domestic PEPs** are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.
- **Persons** who are or have been entrusted with a prominent function by an international organization refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions.

The definition of PEPs is not intended to cover middle ranking or junior individuals in the foregoing categories. PEPs are seen as higher-risk customers by financial institutions (FIs) and DNFBPs because PEPs have more opportunities than ordinary citizens to acquire assets through unlawful means (such as embezzlement and bribe-taking) and thus, are more likely to launder money.



Due to their position and influence, it is recognised that many PEPs are in positions that potentially can be abused for the purpose of committing money laundering (ML) offences and relate predicate offences, including corruption and bribery, as well as conducting activity related to terrorist financing (TF).

The Financial Action Task Force Guidances on PEPs

⁵ Ibid., p. 9.

⁶ Chakravarti, A., (2020). (online). Trumpworld's Corruption Is as Globalized as the Ultra-Rich the President Mingles with Elliott Broidy and others are connected to globe-spanning scandals. Available at <https://foreignpolicy.com/2020/10/12/trumpworld-corruption-elliott-broidy-ultra-rich/>, accessed 10 January 2021.

FATF recommends additional AML/CFT measures to monitor PEP financial transactions while taking reasonable measures to establish the source of their wealth and the origin of funds going into their account.

In relation to foreign PEPs (whether as a customer or beneficial owner), FIs are required to perform additional customer due diligence measures, that (FATF, 2023b):

- have appropriate risk-management systems in place to determine whether the customer or the beneficial owner is a PEP;
- obtain senior management approval for establishing (or continuing, for existing customers) such business relationships;
- take reasonable measures to establish the source of wealth and source of funds; and
- conduct enhanced ongoing monitoring of the business relationship.

FIs are required to take reasonable measures to determine whether a customer or beneficial owner is a domestic PEP or a person who is or has been entrusted with a prominent function by an international organization. In cases of a higher risk business relationship with such persons, FIs should be required to apply the measures referred to in paragraphs (b), (c) and (d). The requirements for all types of PEP should also apply to family members or close associates of such PEPs.

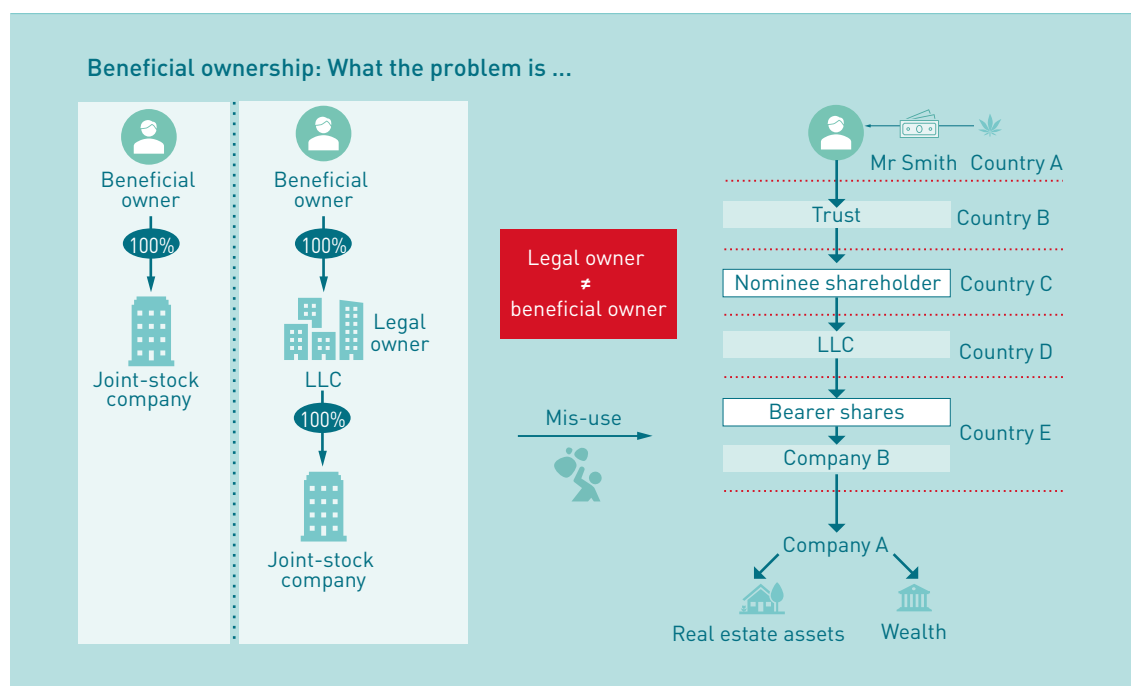
Beneficial ownership (BO)

The beneficial owner is defined as the natural (living) person who ultimately owns or controls the legal entity or the legal arrangement or benefits from its assets; or the person on whose behalf a transaction is being conducted; or both. Beneficial owners also include those persons who exercise ultimate effective control over a legal entity or arrangement. By definition, a *beneficial owner* has to be a *natural, living person*, not a company or trust or any other legal structure, but *an individual*.

BO is also different from legal ownership in that it is not solely related to the amount or percentage of a shareholding or other legal ownership an individual has. Rather, it relates to the exercise of direct or indirect control over the entity and/or its structure.

Control and legal ownership can often, but not always, lie in the same hands. BO is also concerned with questions such as: who derives benefit? and, on whose behalf are transactions being undertaken? In situations where even if someone does not legally own or directly control the entity or structure but is, for example, acting through formal or informal nominees (such as associates, family members or other “front” men), such questions create clarity. There is some variation in the definition of BO among the countries being analysed, which sets the benchmark for professional intermediaries, FIs and government departments, in terms of who they have to identify (and verify) as the beneficial owner.

Figure 2: The difference between the beneficial owner and the legal owner



Source: OECD GF Toolkit, 2019.

The concept of (ultimate) beneficial owners or controllers has become increasingly important internationally as it plays a central role in transparency, the integrity of the financial sector, and law enforcement efforts. Beneficial owners are always natural persons who ultimately own or control a legal entity or arrangement, such as a company, a trust, a foundation, and so forth. A simple example (depicted in Figure 2 on the left), demonstrates how the use of a legal entity or arrangement can obscure the identity of a beneficial owner. When an individual is the sole shareholder of a company and controls it directly, that individual is the beneficial owner of the company. However, there may be more layers involved in the ownership structure – perhaps a chain of entities between a legal vehicle and its beneficial owner (as illustrated in Figure 2 on the right) – which shows additional layers between the beneficial owner, and their assets and wealth. These added layers increase the opacity and complexity of understanding who the ultimate beneficial owner is, who ultimately controls and directs the various legal entities. Thus, the concept of “beneficial ownership” is at the heart of hidden money trails and cuts across different types of IFFs.

The FATF Recommendations are the most widely established international standards for ensuring and promoting BO information. The FATF defines beneficiaries and beneficial owners differently, and looks into whether a clarification of the definition of beneficial owner in the case of legal arrangements is warranted.

A separate definition could further clarify the concept of ownership and control in the context of legal arrangements. Under this approach, BO information could include the identity of each: (i) settlor; (ii) trustee(s); (iii) protector (if any); (iv) beneficiary, or where applicable, class of beneficiaries or objects of a power; and (v) other natural person(s) exercising ultimate effective control over the arrangement.

In the case of a legal arrangement similar to an express trust, beneficial owner refers to the natural person(s) holding an equivalent position to those referred above. When the trustee and any other party to the legal arrangement is a legal person, the beneficial owner of that legal person should be identified. In the current definition included in FATF, the “beneficial owner” refers to *the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement Only a natural person can be an ultimate beneficial owner, and more than one natural person can be the ultimate beneficial owner of a given legal person or arrangement.*⁷

The 2014 *FATF Guidance: Transparency and Beneficial Ownership*, suggests that the essence of the definition ought to extend beyond legal ownership and control to consider the notion of ultimate (i.e. *actual*) ownership and control.⁸ In the 2023 FATF Guidance, in the context of legal persons, beneficial owner refers to the natural person(s) who *ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted*. It also includes those natural persons who exercise ultimate effective control over a legal person. Only a natural person can be an ultimate beneficial owner, and more than one natural person can be the ultimate beneficial owner of a given legal person. In the context of legal arrangements, beneficial owner includes: (i) the settlor(s); (ii) the trustee(s); (iii) the protector(s) (if any); (iv) each beneficiary, or where applicable, the class of beneficiaries and objects of a power; and (v) any other natural person(s) exercising ultimate effective control over the arrangement. In the case of a legal arrangement similar to an express trust, beneficial owner refers to the natural person(s) holding an equivalent position to those referred above. When the trustee and any other party to the legal arrangement is a legal person, the beneficial owner of that legal person should be identified.⁹

The FATF definition focuses on:

- the natural (not legal) persons.
- those who really exert effective control over it (whether or not they occupy formal positions within that legal person), rather than just the (natural or legal) persons who are legally (on paper) entitled to do so.
- own or control either through direct or indirect means.
- individuals that are central to a transaction being conducted even where the transaction has been deliberately structured to avoid control or ownership of the customer but to retain the benefit of the transaction.
- receive the economic benefit (on whose behalf a transaction is conducted).

The definition excludes:

- references to entities other than natural persons;
- the notion of intermediary entities, whether persons, legal persons, or legal arrangements;

7 <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/R25-public-consultation.html#:~:text=%E2%80%9CBeneficial%20owner%20refers%20to%20the,a%20legal%20person%20or%20arrangement.>

8 FATF (2014). *Guidance on Transparency and Beneficial Ownership*. <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-transparency-beneficial-ownership.pdf>

9 FATF. (2023a). *Guidance on Beneficial Ownership for Legal Persons*. Available at [Guidance on Transparency and Beneficial Ownership \(fatf-gafi.org\)](https://www.fatf-gafi.org).

- the need to have a threshold;
- a prescribed threshold for determining controlling participation;
- the requirement to verify the identity of beneficial owners; and
- whether all beneficial owners need to be identified or only those who meet or exceed a certain level of ownership or control.

The FATF *does not mandate a threshold for determining controlling participation*, although a high threshold is unlikely to satisfy the FATF Standard. Each FATF member country takes international norms and national contextual realities into account and *defines its own threshold applicable* for its jurisdiction. The most common threshold is 25 per cent ownership or control. “Thresholds should be set sufficiently low so that all relevant individuals with beneficial ownership and control interests are included in declarations. A risk-based approach should be considered to set lower thresholds for particular sectors, industries, or people, depending on the policy objectives set. Using sufficiently low thresholds to determine ownership or control reduces the risk that someone with relevant ownership or control remains hidden. Extremely low thresholds may become too labour or cost-intensive without providing useful insight into significant ownership or control. A risk-based approach can help determine appropriate thresholds that balance these factors, bearing in mind the country’s policy aims. Lower thresholds may be warranted for high-risk sectors, industries, and people.”¹⁰

The challenge arises in situations where the ownership chain involves legal persons and legal arrangements spread across multiple jurisdictions, or complex networks comprising multiple layers of corporate vehicles. In such cases, ensuring that the beneficial owner information is adequate, accurate, and up-to-date can be particularly challenging. Furthermore, issues related to legal professional privilege and professional secrecy can also pose obstacles to accessing information about corporate vehicles, as lawyers often act as trustees or nominees, and the scope of legal professional privilege varies across different countries and types of legal professionals.

Review of PEP and BO transparency

The Panama, Pandora, and FinCEN papers exposed how anonymously-owned companies in offshore centres are used by tax evaders and criminals, including politicians. These entities hide identities and financial activities, complicating authority investigations. The Pandora papers, for instance, revealed that politicians and elites owned up to £4 billion in UK properties anonymously¹¹ In 2017, the former British Prime Minister Tony Blair and his wife became the owners of a £6.5 million office building in London. They set up a UK real estate leasing company, which acquired a British Virgin Islands holding company (Romanstone International Limited) that owns the property. About £312,000 in stamp duty was avoided as they were buying a business,

10 Open Ownership (2023). The Open Ownership Principles for Effective Beneficial Ownership Disclosure. January 2023. Available at: [oo-guidance-open-ownership-principles-2023-01.pdf](https://cdn.oo-guidance-open-ownership-principles-2023-01.pdf) (cdn.ngo)

11 Goodley, S., Harding, L., Mason, R., & Davies, H. (2021). Revealed: how Tory co-chair’s offshore film company indirectly benefited from £121k tax credits. *The Guardian*.

not a property. The offshore company itself was a subsidiary of another offshore firm (Riverton Capital Holding S.A) owned by the family of Zayed bin Rashid Alzayani, Bahrain's Minister of Industry, Commerce and Tourism.¹² According to data from Pandora papers, the ultimate beneficial owner of the offshore company Romanstone International Limited are: Honourable Anthony Charles Lynton Blair, Cherie Blair, Hamid Rashid Abdulrahman Alzayani, Khalid Rashid Shaikh Abdulrahman Alzayani, Zayed Rashed Shaikh Abdulrahman Alzayani. The last three are shareholders of Riverton Capital Holding S.A, as revealed by the Panama Papers.¹³

Globally, there's a significant movement towards enhancing BOT as a strategy to combat tax evasion and IFFs. This effort, recognized and advocated by organizations such as FATF, Inter-American Development Bank (IDB), Organisation for Economic Co-operation and Development (OECD), and the World Bank (WB), has led to many countries implementing BOT measures designed to uncover the true ownership of corporations and entities, thereby curbing financial crimes and promoting economic integrity.

The updated FATF Recommendations include new requirements for countries to enhance transparency and the availability of BO information, emphasizing the importance of ensuring the adequacy, accuracy, and up-to-date nature of BO information for legal arrangements, as well as the powers of competent authorities to access this information and the maintenance of such information by trustees and equivalent positions.¹⁴ These include the following:

- **Adequate information:** Adequate information refers to information that is sufficient to identify the natural persons who are the beneficial owner(s) and their role in the legal arrangement.
- **Accurate information:** Accurate information is information that has been verified to confirm its accuracy by verifying the identity and status of the beneficial owner using reliable documents, data, or information. The extent of verification measures may vary according to the specific level of risk.
- **Up-to-date information:** Up-to-date information is information that is as current as possible and is updated within a reasonable period following any change.
- **Powers of competent authorities:** Competent authorities, particularly law enforcement authorities and Financial Intelligence Units (FIUs), should have all the necessary powers to obtain timely access to information held by trustees, persons holding equivalent positions in similar legal arrangements, and other parties, including information held by financial institutions and DNFBPs.
- **Maintenance of information:** Trustees and persons holding equivalent positions in similar legal arrangements should be required to maintain the information for at least five years after their involvement with the trust or similar legal arrangement ceases. Other authorities, persons, and entities may also be encouraged to maintain the information for at least five years.

12 Ibid.

13 See <https://offshoreleaks.icij.org/nodes/240024734>, <https://offshoreleaks.icij.org/nodes/240025610> and <https://offshoreleaks.icij.org/nodes/10144712>

14 FATF (2023b). *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*. FATF. Available at www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html

- **Access to information:** Countries should consider measures to facilitate access to information held on trusts or other similar legal arrangements by other authorities, persons, and entities, as well as by financial institutions and DNFBPs undertaking the requirements set out in Recommendations 10 and 22.
- **Legal recognition of trusts:** Countries are not required to give legal recognition to trusts. However, appropriate obligations should exist for trustees, such as through common law or case law.

The implementation of BOT varies by country, reflecting different legal frameworks and economic contexts, but the overarching goal remains to ensure greater financial transparency and accountability in the global financial system.

Stakeholder responses to the public BO register is significant. In the United Kingdom, various organizations, including law enforcement, FIs, and civil societies, actively use the register, as evidenced by a 2019 study.¹⁵ Following its introduction, the United Kingdom noted a substantial decline in Scottish Limited Partnerships registrations, a known secrecy vehicle, dropping 80 per cent by the end of 2017.¹⁶ The OpenLux investigation in Luxembourg also revealed the register's effectiveness in uncovering suspicious activities.¹⁷

However, there are deficiencies in the implementation of the ownership transparency in most countries that might limit the effectiveness of the register. First, the directive leaves member states with discretion. "Legitimate interest" for accessing the register is a vague concept and can reduce the effect of public scrutiny. Entities that are only a branch or a legally dependent entity of a foreign company may be exempt from reporting requirements.¹⁸ Second, failure in information verification enables the exploitation of loopholes or submission of false information. Also, the 25 per cent threshold can be circumvented as, for example, multiple layers of interlocking shareholding links (so-called Chinese boxes) make it difficult to identify the real beneficial owner.¹⁹ In addition, circular ownership structures can be used to make sure an investor's shares or voting rights fall below the threshold of 25 per cent while the investor controls the company.^{20, 21} Global Witness, for instance, evaluated the UK register in 2019 and revealed that 336,224 companies simply say they have no beneficial owner. In Luxembourg, more than half of the firms do not declare beneficial owners, while others give conflicting information.²²

15 BEIS. (2019). Review of the implementation of the PSC Register. *BEIS Research Paper* Number 2019/005.

16 Global Witness. (2018). *The Companies We Keep: What the UK's open data register actually tells us about company ownership*.

17 See the OpenLux investigation and database (<https://www.occrp.org/en/openlux/>), which combines data from the Luxembourg company register and the Luxembourg beneficial ownership register.

18 For example, in the Netherlands, formally foreign legal entities are not legal entities incorporated under Dutch law, they will not be obligated to register their UBOs in the Netherlands. The same will apply to branches of foreign entities registered in the Netherlands.

19 Transcrime. (2018). *Mapping the Risk of Serious and Organised Crime Infiltration in Europe – Final Report of the MORE Project*.

20 Bosisio, A., Carbone, C., Jofre, M., Riccardi, M., & Guastamacchia, S. (2021). *Developing a Tool to Assess Corruption Risk factors in firms' Ownership Structures – Final report of the DATACROS Project*.

21 Also see <https://www.taxjustice.net/2019/09/06/more-beneficial-ownership-loopholes-to-plug-circular-ownership-control-with-little-ownership-and-companies-as-parties-to-the-trust/>

22 White, J. (2021). OpenLux shows failures of beneficial ownership registers. *International Tax Review*.

PEP and BOT toolkit

This section outlines **seven core pillars or frameworks of the toolkit**, drawing on **the twelve principles for effective BO disclosure derived from Open Ownership**, which are designed to make published data easy to use, accurate and interoperable. In addition, the toolkit incorporates additional elements creating an end-to-end BOT and PEP scrutiny value chain for country governments.

The core pillars of this guiding framework for an effective BOT and PEP scrutiny toolkit, address the following focal areas:

- reform of the legal framework;
- development of a national strategy, action plan and agenda;
- creation of technical systems and tools for analysis;
- development of the policies and procedures to collect, store, verify, update, analyse and share information;
- mechanisms to monitor, track and trace beneficial owners and scrutinize PEPs;
- highlight the skills, resources and capacity required; and
- the communication, publication of data and collaboration to share information within a country's institutions and across institutions in other jurisdictions.

The seven pillars of the toolkit are illustrated in the figure below.

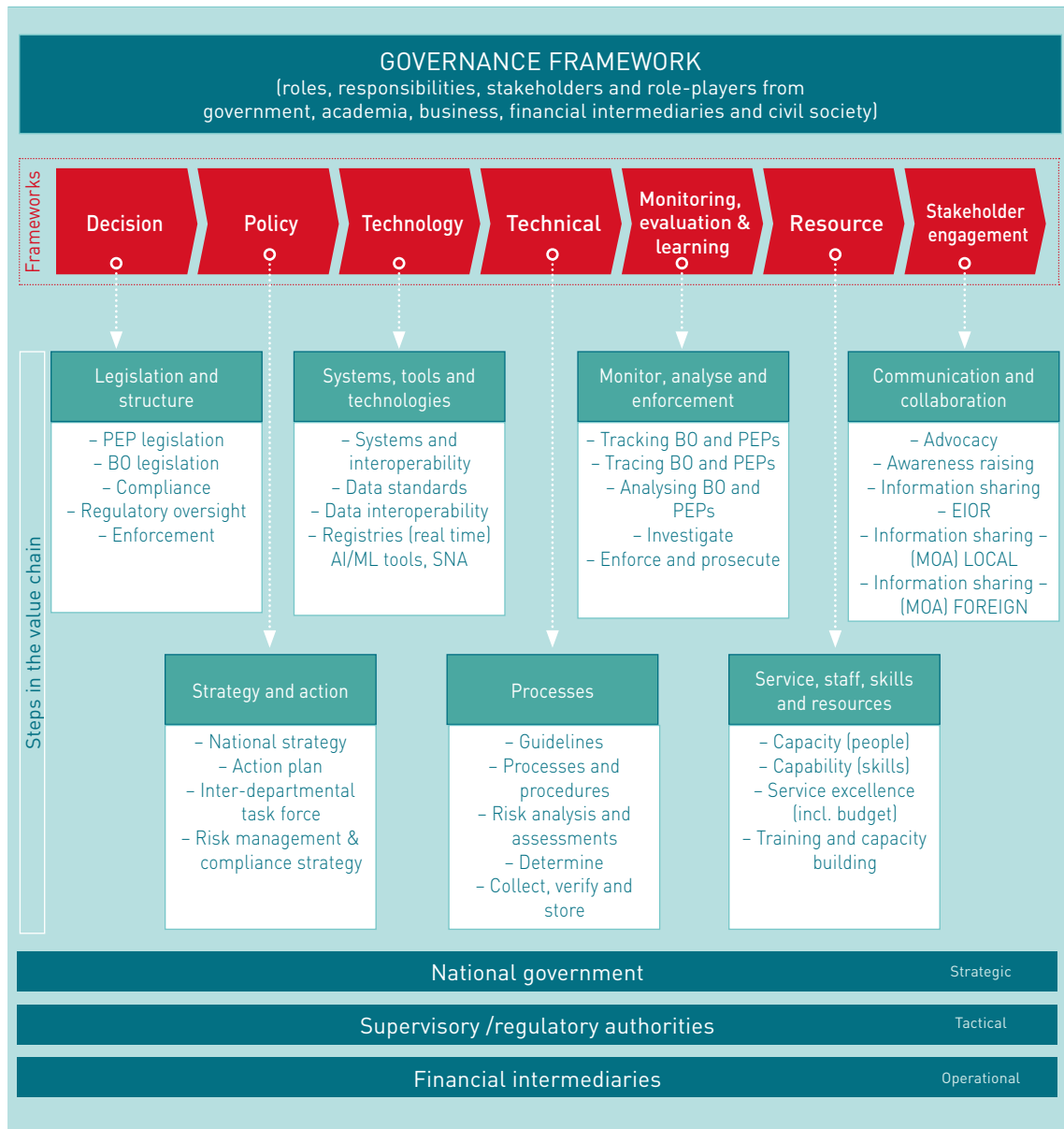
Figure 3: Core pillars of the PEP scrutiny and BOT toolkit



Although work on each area is often undertaken by different experts and departments, these seven components must work together in a synergistic manner for a holistic, integrated BOT and PEP scrutiny toolkit that effectively curbs ML, terror and proliferation financing, ensuring that the data can be usefully applied across the board.

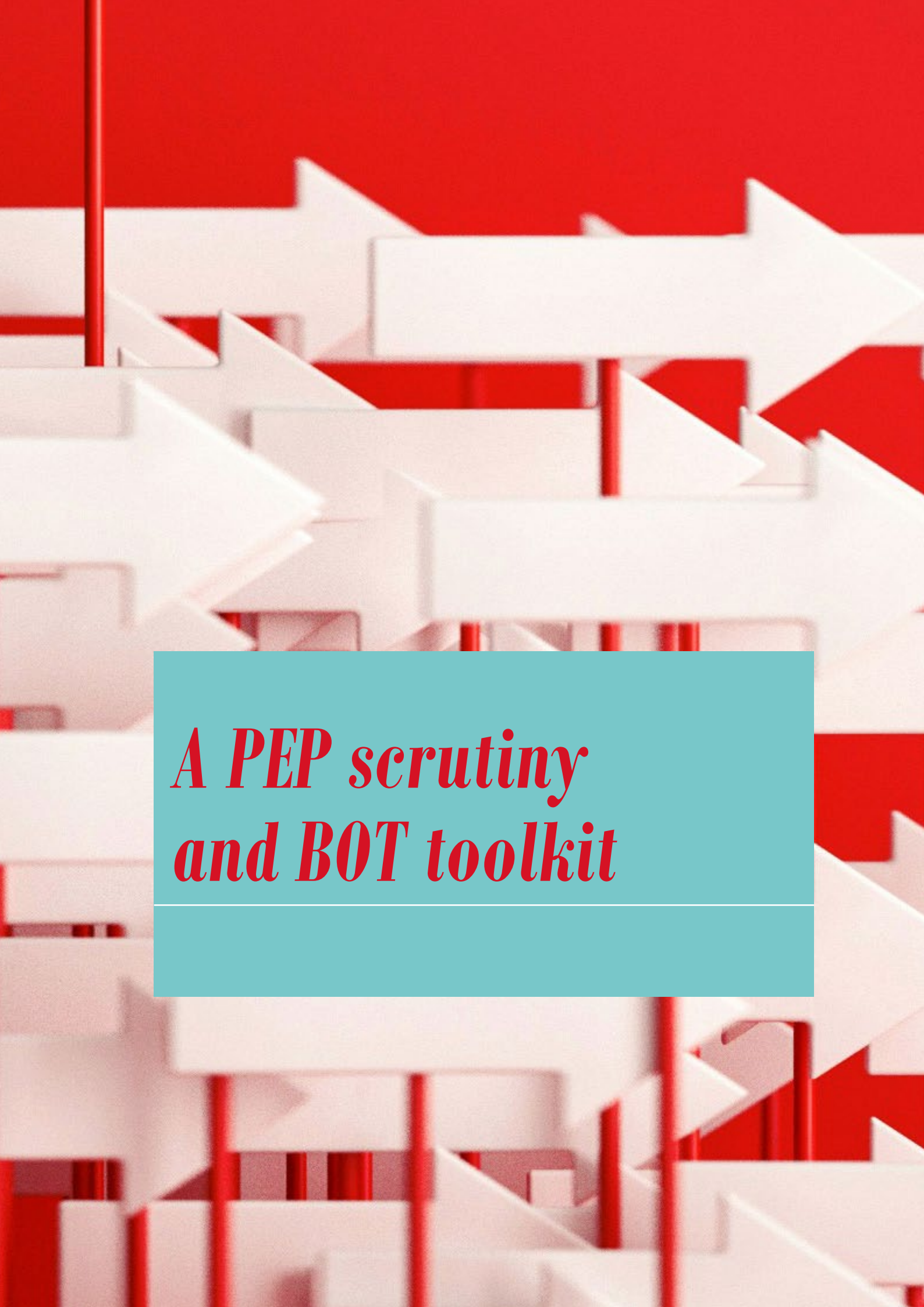
The figure below highlights the various steps in the value chain necessary to build a comprehensive, integrated BOT and PEP scrutiny mechanism.

Figure 4: Components of the seven pillar value chain – PEP scrutiny and BOT toolkit



In the section that follows, each of these will be discussed in detail, drawing on the elements that are relevant from the Open Ownership principles.





*A PEP scrutiny
and BOT toolkit*

The following chapter explores the seven core pillars or frameworks of the toolkit, drawing on the twelve principles for effective BO disclosure derived from Open Ownership, which are designed to make published data easy to use, accurate and interoperable.

Legislation and structure: decision framework

The initial step of implementing a BO and PEP scrutiny tool involves comprehensive legislative, regulatory, and policy reforms and amendments. This commitment requires a thorough understanding of the implications, necessitating political will and dedication to incorporate these changes into existing legislation or develop entirely new legislation. However, legislative amendments are just the beginning, as successful implementation demands extensive work, coordination, collaboration, and operational execution.

Legislation and regulation

The process of amending legislation and introducing regulatory reforms should be spearheaded by a championing ministry or lead government agency tasked with implementing a holistic and comprehensive PEP scrutiny and BO disclosure mechanism. This ministry or government should play a pivotal role in ensuring the effective integration of legislative and regulatory changes into the existing framework.

BO is a key component of various international standards and guidelines, including those established by the Extractives Industry Transparency Initiative (EITI), FATF, the European Union (EU), the Group of 20 (G20), and the OECD. When defining BO, it is imperative to ensure that it addresses all pertinent forms of ownership and control, thereby reducing the likelihood of individuals exploiting and abusing a country's economy and natural resources. The definition should:

- Specify that a beneficial owner must be a natural person.
- Encompass both ownership and control interests.
- Include both indirect and direct interests.
- Feature low thresholds for triggering BO disclosure, ensuring the inclusion of all individuals with BO and control interests in disclosures.
- Apply special consideration to ownership by PEPs.
- Utilize absolute values, rather than ranges, when reporting the percentage of ownership or control that a beneficial owner holds.

An effective definition is likely to combine a comprehensive general description of BO, supplemented by a non-exhaustive list of examples illustrating how these interests can be held, in the local context. Where feasible, definitions should be harmonized regionally and internationally, or similar minimum standards should be adopted to ensure consistency and effectiveness across jurisdictions.

The legislation pertaining to PEPs must feature a comprehensive definition that encompasses all individuals with influence, whether at a domestic or international level. This inclusive definition should empower government institutions to utilize the information for curbing tender fraud and corruption, while providing financial institutions and DNFBPs with the framework to comply with the FATF 40+ AML/CFT recommendations, UNCAC requirements, and other relevant standards.

Harmonizing various pieces of legislation is essential to establish consistent definitions of PEPs and beneficial owners across different sectors, aligning with the government's objectives in AML/CFT, addressing IFFs, and combating corruption. This harmonization process encompasses a wide array of sectors, including the extractive industry, financial services, investment, banking, insurance, tax and customs, AML/CFT, and other relevant areas. Additionally, it involves aligning with international standards such as the UNCAC and the FATF 40+ recommendations, among others.

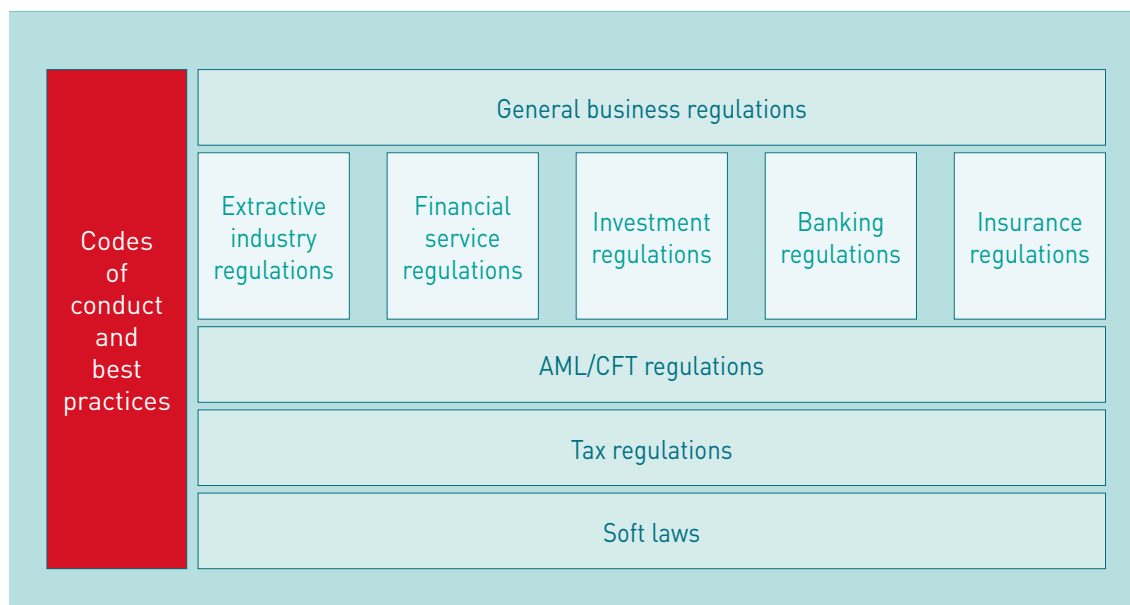
The following questions and perspectives need to be considered to effectively amend legislation:

- Scanning the existing legislation, what legislative changes are required for BOT? This should include some of the legislation relating to companies, partnerships, trusts, AML/CFT, privacy and data protection, non-profits, banking licensing, to mention a few.
- Who should be involved in developing the legal framework?
- Is BO information to be disclosed publicly?
- Who is responsible for disclosing information on BO and PEPs with BO?
- Who will use the BO register, and what data do they need to achieve your intended policy impact? Should open data be included in the law? Should this include public access?
- Who is responsible for managing the register?
- If it is the state, then whose mandate is it? If not, then who is responsible for this outside of government (e.g. civil society? each financial institution? DNFBP?)
- What type of register will be put in place and where?
- What data privacy and data protection provisions need to be taken into account?
- Will the database be located in one place or draw on information from multiple sources? What are the governance and technological arrangements for this? What legislative requirements are necessary to ensure that data can be shared and is interoperable?
- What are the options of a shared BO utility?
- Which legal vehicles will be subject to disclosure requirements? Are there any legitimate exemptions? What should be collected? How regularly will information be collected, managed and updated? How will it be verified? And by whom?
- How can the legal framework facilitate investigations?
- What is the role of the legal framework toolkit on monitoring, tracking, tracing and enforcement?

Figure 5 indicates that while there are specific regulatory requirements for different sectors (like extractive industries or financial services), there are also broader regulations that cut across all sectors (like AML/CFT and tax regulations). Soft law, while not legally binding, may inform or complement the formal regulations. These regulations should be in alignment with recognized best practices and ethical standards in the industry.

- **General business regulations:** This is the overarching category that likely includes general principles and rules that apply to all business activities regardless of the specific industry.
- **Sector-specific regulations:**
 - **Extractive industry:** Rules and guidelines that govern the extraction industries, such as mining, oil, and gas.
 - **Financial services:** Regulations specific to the financial services sector, which may include banking, investments, stock exchanges and insurance companies.
 - **Investment:** Laws and regulations that apply to investment practices and entities such as investment banks, fund managers, stockbrokers and investors.
 - **Banking regulations:** This includes regulations that govern the operations of banks and financial institutions.
 - **Insurance regulation:** Rules and standards for the insurance industry, overseeing how insurance products are sold and managed.
- **Cross-sector regulations:**
 - **AML/CFT regulation:** Regulations that are designed to prevent illegal financial activities across all sectors.
 - **Tax regulation:** Laws that dictate tax obligations and procedures for businesses and individuals, applicable across all sectors.
 - **Soft law:** Non-binding guidelines, principles, or standards that influence or guide business practices and regulatory compliance across all areas.

Figure 5: Harmonization of various pieces of legislation and regulations



Furthermore, the legislative and regulatory reforms should aim to establish a comprehensive framework that not only defines PEPs and beneficial owners but also outlines the obligations and responsibilities of entities in identifying and disclosing this information. This framework should encompass mechanisms for ongoing monitoring, reporting, and ensuring compliance with the established standards. Additionally, it should address the need for transparency and accessibility of BO information, enabling competent authorities to swiftly access and utilize this critical data for AML/CFT efforts and international cooperation.

Policy makers are encouraged to map out the mandates of relevant agencies, such as tax authorities and law enforcement agencies (LEAs), to identify overlap, interdependencies, and opportunities for closer coordination. A strong public policy stance on inter-agency cooperation is vital to overcome legal, operational, and cultural barriers. Similarly, an appropriate legal framework free from unreasonable and disproportionate legal barriers to the exchange of information is also necessary.

Compliance, regulatory oversight, and enforcement

While legislative amendments provide the foundation for the compliance framework, it is meaningless without effective implementation. The overseeing Ministry, as the custodian of these legislative changes, is responsible for executing an action plan to bring the legislation to life. This involves establishing mechanisms for monitoring compliance and imposing sanctions or penalties on non-compliant entities. Furthermore, there is a need to communicate the legislation to the public in a clear and accessible manner, to ensure widespread understanding and compliance.

In the context of PEP and BO disclosure requirements imposed on government institutions, corporate entities, legal bodies, or members of the public, the overseeing Ministry or lead government agency must oversee and ensure adherence to these mandates. This entails the collection, maintenance, updating, monitoring, and analysis of PEP and BO information. If this information is not centrally collected and stored, other ministries and government institutions should be mandated to do so, with a clear legal directive to share this information for compliance, monitoring, and enforcement purposes.

The importance of effective regulatory oversight and enforcement cannot be overstated. The overseeing ministry is responsible for implementing legislative amendments, developing policies, regulations, practice notes, and guidelines to ensure compliance with the legislation. It must also ensure that the legislation and regulations are responsive to the changing world and environment. This includes incorporating lessons learned from instances of non-compliance among government members or the public, addressing any flaws which hinder compliance or create excessive regulatory burdens, identifying key gaps in the legislation, and implementing remedial regulatory reforms to tackle these challenges.

Effective monitoring of compliance with the legislation should be supported by an investigative and enforcement capability within the overseeing ministry. This capability is crucial for imposing sanctions or penalties in cases of non-compliance, thereby ensuring the effectiveness and integrity of the regulatory framework. The sanctions or penalties imposed should be effective, proportionate, and dissuasive, serving as a deterrent to non-compliant entities.

International cooperation and coordination

International cooperation and coordination are essential for combating ML and TF. Countries should provide the widest possible range of international cooperation in relation to basic and BO

information, as set out in FATF Recommendations 37 and 40.²³ This includes facilitating access by foreign competent authorities to basic information held by company registries, exchanging information on shareholders, and using their powers to obtain BO information on behalf of foreign counterparts. Countries should also monitor the quality of assistance they receive from other countries in response to similar requests and others such as requests for assistance in locating beneficial owners residing abroad.

Legal frameworks that enable and mandate information sharing, establish legislative mandates for reporting suspicious cases, and address legal barriers to international cooperation to enhance collaboration between tax authorities and LEAs in combating financial crimes include the following:²⁴

- **Domestic level:** Establishing a framework that encourages, authorizes, or mandates tax authorities to share certain information with LEAs, and vice versa, is vital due to the strong link between tax crimes and other financial crimes. Tax authorities and/or FIUs should join forces to have a multi-pronged approach to fighting crimes, for instance by establishing a legislative mandate to report suspicious cases to the appropriate LEAs. An appropriate legal framework is a building block for successful inter-agency cooperation, including creating the overall framework for information sharing and specific provisions for BO. Domestic laws must enable information sharing between agencies in the same jurisdiction, and it is worthwhile to consider laws that better enable information gathering, such as the inclusion of tax crimes as predicate offenses to money laundering and mandatory disclosure rules.
- **International level:** Overcoming legal barriers to international cooperation between the relevant agencies and the tax authorities and FIUs of counterpart countries is essential. Developing a legislative framework formally linking tax crimes to broader financial crimes, enacting and implementing legislation authorizing or mandating tax authorities to disclose transactions found during tax audits that facilitate the commission of financial crimes, and enacting and implementing legislation authorizing or mandating LEAs to disclose information found during criminal investigations related to tax evasion are recommended to enhance international cooperation.

Strategy and action: policy framework

The next step draws on the legislative mandate given to a particular ministry responsible for reforming the policy agenda of government to implement a holistic and comprehensive PEP scrutiny and BO disclosure mechanism for the country. In this case, the legislative steps relate to definitions that are required to establish the legal basis for developing and implementing a comprehensive national strategy, ensuring that the existing legal framework creates the mandate that supports the necessary processes for stakeholder consultation and the development of a national strategy.

23 Op.cit., FATF (2023b).

24 Brun, J.-P., Gomez, A., Julien, R., Ndubai, J., Owens, J., Rao, S., & Soto, Y. (2022). Taxing Crime: A Whole-of-Government Approach to Fighting Corruption, Money Laundering, and Tax Crimes. In *Taxing Crime: A Whole-of-Government Approach to Fighting Corruption, Money Laundering, and Tax Crimes*. <https://doi.org/10.1596/978-1-4648-1873-8>.

In some countries, depending on the legal and regulatory framework, the national strategy could precede the legislative and regulatory framework being developed and promulgated into law.

National strategy

The development of a national strategy for scrutinizing PEPs and ensuring BO disclosure is a critical responsibility of the overseeing ministry or lead government institution. This mandate is derived from legislation and requires thorough research to guide the implementation of BOT and PEP disclosure mechanisms within the country's specific context. While international best practices can provide valuable insights, the strategy must be adapted to the country's unique circumstances. Collaboration with international organizations and civil society groups, such as Open Ownership, can provide valuable support in shaping the strategy and addressing critical considerations and processes. Other resources that could assist or guide include the FATF, Egmont,²⁵ UNODC, UNCAC, World Bank, OECD, EU, the Canadian, Nigerian, German and UK governments, to mention a few.

The national strategy should include the following:

- A vision, mission statement and goals for a BOT and PEP disclosure mechanism.
- Clear aims, objectives, and outcomes.
- A stakeholder map of all the role-players and stakeholders and roles and responsibilities of all parties involved.
- A list of participating stakeholders (public and private) who will participate in the National Advisory Committee.

Once the strategy has been developed, it needs to be adopted by government. This process varies among countries. For example, in some countries the strategy might need a cabinet memorandum for its adoption; in others, mere approval from the Minister could suffice. The end result should include a Ministerial or cabinet mandate for core participating government departments to form part of the advisory committee and establish an inter-department task force or working group, necessary to promote coordination and cooperative governance. Existing structures could be leveraged to avoid duplication of work and resources. If there is an existing committee or inter-departmental task force, the strategy should be added into their roles, and the responsibilities and mandate should be augmented accordingly.

Widespread dissemination of the strategy beyond government is essential, supported by a comprehensive communication plan to foster awareness, advocacy, and broad-based adoption of the strategy. This should include both an internal communication plan for government and an external communication plan for the public or private sector.

Capacity building and training initiatives should be prioritized by the overseeing ministry to equip relevant stakeholders with the necessary knowledge and skills to effectively implement

²⁵ <https://egmontgroup.org>.

the national strategy. This may involve conducting workshops, seminars, and targeted training programmes to enhance understanding and compliance with the strategy's objectives.

The national strategy should incorporate robust monitoring and evaluation mechanisms to track progress, identify challenges, and make informed adjustments as necessary. Regular assessments and reporting should be conducted to ensure the strategy's effectiveness and relevance over time.

In addition to collaborating with international organizations and international civil society groups, the government should also consider engaging with other governments that have successfully implemented BOT and PEP disclosure mechanisms. This can provide valuable insights and support in shaping the strategy and addressing critical considerations and processes.

Inter-Departmental Task Force

Given the multitude of stakeholders involved in BOT and PEP scrutiny, establishing an Inter-Departmental Task Force is advisable. This Task Force should ensure a common vision and understanding across government departments, the private sector, and civil society. Its responsibilities can include fostering collaboration, facilitating information sharing between institutions, mitigating and managing risks, ensuring compliance, conducting analysis, and enforcing measures across the entire value chain for all participating ministries.

Furthermore, the Task Force should possess the capability to identify challenges and issues, offering iterative and adaptive solutions to ensure the successful implementation of the national strategy and action plan. Additionally, it should provide guidance for the development and communication of regulations, policy directives, and practice notes, both internally within the government and externally to the public.

The establishment of this Task Force is crucial for promoting a cohesive approach to BOT and PEP scrutiny. By fostering collaboration and information sharing, it can effectively address the complexities and challenges inherent in these processes. Moreover, its role in risk mitigation, compliance, and enforcement will contribute to the overall effectiveness of the national strategy and action plan.

In addition, the Task Force's ability to provide guidance on regulatory and policy matters ensures that the necessary frameworks and directives are in place to support the implementation of the strategy. This proactive approach not only facilitates internal coordination but also enhances transparency and accountability in the communication of regulations and directives to the public.

By fulfilling these multifaceted responsibilities, the Inter-Departmental Task Force plays a pivotal role in driving the successful execution of the national strategy, ultimately contributing to the overarching objectives of promoting transparency and integrity in PEP scrutiny and BOT.

Action plan

The development of an action plan stemming from the national strategy is a critical step that falls under the purview of the overseeing ministry. Depending on the strategy and the delineated roles and responsibilities of the various stakeholders, committees, or sub-committees or working groups, this responsibility may be delegated to the Task Force, which functions as the operational arm of the overseeing ministry.

This action plan is expected to delineate the key objectives and outcomes to be accomplished, incorporating detailed, measurable, and concrete action steps with clear key performance indicators. A responsible department or entity must be appointed to oversee the execution of the action plan. In formulating the action plan, due consideration should be given to the various components of the value chain. It should comprehensively outline the roles, responsibilities, actions, and anticipated outcomes necessary to establish a robust mechanism for ensuring transparency in scrutinizing PEPs and BO within the country.

This comprehensive approach will ensure that the action plan is effectively implemented, thereby contributing to the overarching goal of enhancing transparency and accountability in the country's financial and governance systems.

Risk management and compliance strategy

One of the pivotal requirements outlined by FATF for FIs and DNFBOs is to establish a robust AML/CFT Risk Management and Compliance Strategy (RM&CS). This critical responsibility may be assigned to the Financial Intelligence Centre (FIC) in certain instances, while in others, it falls under the purview of a supervisory authority overseeing FIs, such as the central bank.

The relevant authority should be tasked with the crucial role of monitoring, inspecting, and enforcing the implementation of the RM&CS, with a specific focus on BO and PEP disclosure. Risks must be comprehensively assessed, and the supervisory authority must have confidence in the efficacy of the mitigating strategies put in place to ensure compliance. The overarching objective is to reduce the risks and threats associated with tax evasion, ML, TF, and corruption stemming from inadequate or insufficient disclosure of BO and PEP information.

In addition, the overseeing ministry and the Inter-Departmental Task Force should also develop their own annual RM&CS to ensure compliance with national laws and to oversee the effective implementation of the national strategy. It should also identify vulnerabilities and enable proactive measures to mitigate the risks and threats.

By developing and implementing comprehensive RM&CS, all relevant entities can proactively address the multifaceted challenges associated with BO and PEP disclosure. This approach not only ensures compliance with international standards but also reinforces the national commitment to combating financial crimes and promoting transparency and integrity in the financial and governance systems.

Implementation of the strategy and action

Having a clear authority and mandate is paramount for the entity tasked with implementing the strategy to combat IFFs. It is imperative that this authority and mandate be explicitly outlined in the organized crime strategy and be firmly linked to the executive branch. This linkage ensures that the entity possesses the requisite power and resources to effectively execute the strategy and be accountable to the highest levels of government. Without a clear authority and mandate, the implementation of the strategy may encounter obstacles such as institutional resistance, resource deficiencies, or inadequate political support. Therefore, establishing a clear authority and mandate for the implementing entity is crucial to ensure the success of the strategy in combating IFFs.²⁶

In the context of strategy implementation, it is anticipated that three levels of structures will be necessary, including a political-level board or council responsible for providing overall direction, a strategy steering group dedicated to propelling cross-sectoral implementation, and an analysis unit positioned alongside the integrated policy and planning unit.²⁷

Furthermore, the successful implementation of the strategy hinges on consultation and buy-in from relevant stakeholders and political leaders. In certain contexts, public announcements and legal endorsement may also be requisite. It is imperative to develop a clear logic delineating objectives and outcomes, as this is vital for outlining corresponding activities, tactics, tools, and techniques aimed at addressing vulnerabilities and achieving the objectives of countering IFFs.

Additionally, the establishment of monitoring and evaluation frameworks is integral to the technical framework, ensuring political accountability, cross-sector coordination, and the implementation of effective monitoring and reporting mechanisms. These measures are essential for assessing the strategy's impact and making any necessary adjustments to enhance its effectiveness in combating IFFs.

Systems, tools and technologies: technology framework

BO transparency and disclosure are essentially about maintaining a record of individuals linked to corporate entities that are transacting financially. This record is a data repository that, in many instances, stitches together information from different sources. As such, the solution to this challenge is largely a technology-based one. Fortunately, significant progress is being made in this space, and governments can draw on the tools developed by civil society organizations such as Open Ownership and the private sector to develop the technology required to gather BO (and PEP) information.

26 UNODC. (2021). *Organized crime strategy toolkit for developing high-impact strategies*. Available at https://www.unodc.org/documents/organized-crime/tools_and_publications/Strategies_Toolkit/OC_Strategy_Toolkit_Ebook.pdf, accessed 20 January 2021.

27 Ibid.

Leveraging existing infrastructure and drawing on such tools already in use to gather BO information is needed. Innovative tools such as Distributed Ledger Technology (DLT) could be particularly useful in this regard. DLT is a decentralized database that enables secure, transparent, and tamper-proof record-keeping. It has the potential to revolutionize the way BO information is collected, stored, and shared. By leveraging DLT, governments can create a secure and transparent platform for collecting and sharing BO information, thereby enhancing transparency and reducing the risks associated with financial crimes.

There are also various other systems and tools. For example, some countries have established central registers of BO information, which can be accessed by competent authorities and FIs. Other countries have implemented Know Your Customer (KYC) and Customer Due Diligence (CDD) requirements, which require financial institutions and DNFBPs to collect and verify BO information.

Systems and interoperability

The effective management of BO and PEPs information requires the use of technology-based solutions that enable the collection, storage, sharing, and analysis of information related to BO and PEPs. To ensure that the information is valuable, can be shared, and be meaningfully used from a counter-IEFs or AML/CFT perspective, the information needs to be in a digitally “structured” and “machine-readable” format that the various technology systems within the public, private, and civil society sectors can read. This requires the establishment of an effective system that can collect, maintain, store, update, verify, analyse, and share information on beneficial owners and PEPs.

Usually, there are numerous databases that store different pockets of information that when joined together, create a comprehensive BO and PEP profile of an individual and the entity they own/control or the position of influence. The software and hardware systems specifications depend entirely on the requirement of the BOT system/solution designed in the national strategy and the requirements stipulated in the legal framework.

Before looking at data standards and what data needs to be shared, it is important to have the technology or system in place to be able to accept and send the data, read, store, manage and update, and finally analyse it.²⁸ It is possible through some agreement to draw on the technology that has already been developed for governments. It might even be possible to adapt the existing system (especially if it is fairly new), by adding a few more rows or questions into the online questionnaire capture the core BO information.

Where information is paper-based or on a legacy system, that information will need to be converted into a digital, machine-readable, or electronic format, which is then stored by the system

²⁸ Open Ownership, for example has a public open data system that can be used by governments (mostly free of charge). There are hardware and data charges associated with such a system but are relatively small. Other countries have embarked on their own systems and data gathering forms, from Kenya, to Nigeria, Denmark, the UK, the Ukraine, and even South Africa (linked to the companies registry) to mention a few.

(possibly the company register). This information can then be shared by either transferring the file electronically to an approved/authorized user, other public or private entities (to their systems), or possibly on a government website portal (where the data is open and freely available online).

Deciding on the systems and technology requirements is a complex exercise, and private sectors or civil society organizations do provide technical solutions to some of the problems. However, the Chief Information Officer and their team should be able to provide policy officials with guidance to the system requirements for BO and PEP transparency solution. According to Open Ownership, these basic steps could assist:

- identify the various pieces of information that are required for a comprehensive, integrated, accurate, and unambiguous BO and PEP disclosure system;
- map pieces of information to the existing data sources and highlight where there are gaps in the existing information sources; and
- map out the current systems that collect to the functional requirements for the common data standard.

Establishing an effective system that can collect, maintain, store, update, verify, analyse, and share information on beneficial owners (and PEPs) does require investment; however, it assists in combating IFFs, tax evasion, corruption, ML, and TF. The benefits of the system far outweigh the costs. By leveraging technology-based solutions, governments can enhance transparency, reduce the risks associated with financial crimes, and promote a more secure and stable financial system.

Next, the establishment of standard data formats and structures is crucial for ensuring that information can be exchanged and understood across different platforms. By adopting common data standards, jurisdictions and systems can overcome the challenges posed by differences in data formats, standards, and protocols, ultimately facilitating interoperability and effective information exchange. The establishment of technical working groups is recommended to address interoperability challenges. These groups can focus on identifying and resolving technical issues related to data formats, standards, and protocols, ultimately working towards ensuring compatibility and seamless information exchange.²⁹

Data standards

Beneficial ownership (BO)

The collection of BO data should be comprehensive, covering three main areas:

- Individual entities, including both personal owners and PEPS, detailing their roles and involvement;
- Legal structures, encompassing owned companies and in certain scenarios, the ultimate owners such as in state-owned enterprises; and
- In-depth insights into ownership and control dynamics, incorporating specifics like shareholding percentages, voting rights, and governance structures like board membership regulations.

²⁹ Op. cit., Brun, J, et al.

The adoption of a uniform framework like the Beneficial Ownership Data Standard (BODS) is crucial for the import and export information of beneficial owners who own or exercise control in other jurisdictions, and for the effective exchange of this data internationally, between competent authorities and LEAs. This standard is particularly pivotal in cases where ownership or control is indirectly held across multiple entities or jurisdictions, aiding in the creation of a cohesive global data network. Where ownership or control is held indirectly through multiple entities and/or multiple jurisdictions, disclosure of intermediate steps in a chain provide an answer on how BO is operating and enables data to be joined up from different sources and countries across the globe. The ability to link BO information transnationally is essential to realizing the full potential of BOT, exposing networks of IFFs and supporting robust and efficient due diligence in the global economy.

Open Ownership provides extensive support in this field, offering both technical and policy guidance. Version 3 of BODS, developed by Open Ownership,³⁰ includes a range of components such as functional requirements, real-world identifiers, and guidelines for collating and sharing BO information for all forms of legal entities and arrangements (including state-owned enterprises), which are vital in shaping the data schema specification. This expanded approach ensures a more robust and transparent global financial system, promoting accountability and reducing the risk of financial misconduct. The website showcases key resources, including the Open Ownership Principles, which establish standards for effective BO disclosure. These principles are designed to aid governments in executing transparency reforms and to guide international institutions in understanding and supporting such initiatives. Additionally, the site features an overview of the Opening Extractives programme, a collaborative effort with the EITI, furthering these transparency goals.

BODS provides a common data model for importing, exporting, storing, updating and sharing information on BO (including PEPs), capturing their direct and indirect ownership and control of the corporate entity, while also including information pertaining to ownership by an entity or natural person of a trust and/or joint shareholding.

The data model, through the data schema, represents and helps identify the ultimate beneficial owner, or natural person(s), who ultimately benefits from or controls a legal entity. Thus, the data model ensures that:

- key information about the beneficial owner, the disclosing company, and the means through which ownership or control is held is included.
- clear identifiers are used for people and companies.
- key information about PEPs are clearly identified within the data. Ideally, it would be preferable for a separate PEPs register that links up with the BO register, identifying where a PEP has business interests in various legal entities and arrangements.

³⁰ <https://www.OpenOwnership.org/en/>

Specifications

Deciding on the systems and technology requirements is a complex exercise, and Open Ownership does provide technical solutions to some of the problems. However, the Chief Information Officer and their team should be able to provide policy officials with guidance to the system requirements for a BO and PEP transparency disclosure solution. Here are some basic tips that could assist:³¹

- Identify the various pieces of information that are required for a comprehensive, integrated, accurate and unambiguous BO and PEP transparency disclosure system.
- Map pieces of information to the existing data sources and highlight gaps in the existing information sources.
- Map out the current systems that connect to the functional requirements for BODS. This will help identify what changes are required to design a system for capturing BO data.

Functional requirements for BO transparency data standards and systems

BODS can accommodate data from a range of data sources, that is of high quality and can be shared efficiently. “They therefore need to meet the following functional requirements:

- Source systems should keep a full audit log with the source of data and changes made to data;
- Publication systems should assign a unique identifier to each statement produced;
- Publication systems should be able to assert when one statement replaces another;
- Publication systems should be able to produce statements in JSON format;
- Publication systems should be able to validate statements against the JSON schema;
- Statements should be immutable.”

Source: Open Ownership, <http://standard.openownership.org/en/latest/schema/guidance/functional-requirements.html>

- Map any current data to the BODS schema³² which provides a common data model for collecting, storing and sharing information on the beneficial owners (including PEPs) of corporate entities, for the purpose of sharing this information. Whether the country chooses to go the Open Ownership route or not, using BODS will ensure that the information can be shared between different registers in country and from foreign jurisdictions. If BO information is being collected, regardless of whether it is held by government, or private or public, the information can be mapped to the Open Ownership BODS schema using Field Mapper (which is open source and publicly available). The Field Mapper flags where the data differs from BODS and highlights fields where there are gaps in the data being collected as well as fields where added measures are needed such as in-line validation that assists in structuring the data.
- Design the system to import, export, store and update BODS data. Open Ownership provides example data in the JSON format to understand what is required, for single and joint ownership or to update ownership.
- The Chief Information Officer’s team should draw up the technical specification for the system drawing on the Field Mapper and example before commencing on the technical build or amending the existing systems. Note, that country governments can draw on the guidelines on the Open Ownership website, and even request some guidance from Open

³¹ Ibid., amended from Open Ownership.

³² Open Ownership (2021), <http://standard.openownership.org/en/latest/schema/index.html>, accessed 21 January 2021.

Ownership. “Use the example data to help you think through what BO data might look like for different company types and what system specifications you will need in order to collect this information.”³³

- The BODS Schema Person Statement contains PEP information in rows 42–49 in the Field Mapper. While this is an optional element, this should be made compulsory, collecting PEP information which is linked to the BO register.
- Use the same steps above for amending existing systems or developing new systems.
- Commission the work.
- Test and validate the data. When your system is in place, the data outputs can be tested against the Open Ownership BODS schema using their Data Review Tool.³⁴

The schema browser³⁵ provides a way of digging through the schema’s structure, showing how its components and fields fit together. Alternatively, the schema reference³⁶ presents these elements and their descriptions in easy-to-reference tables. Further considerations regarding the validation, publishing, and lifecycle of data are included in the technical guidance.³⁷ More detailed recommendations on structured and interoperable BO data is available at: [oo-briefing-structured-interoperable-BO-data-2022-08_0vKtMx2.pdf \(cdn.ingo.org\)](https://cdn.ingo.org/oo-briefing-structured-interoperable-BO-data-2022-08_0vKtMx2.pdf)

A common data standard makes it easier to import and export information of beneficial owners who own or exercise control in other jurisdictions. Where ownership or control is held indirectly through multiple entities and/or multiple jurisdictions, disclosure of intermediate steps in a chain is helpful. It provides detail about how BO is operating and enables data to be joined up from different sources and countries across the globe. The ability to link BO information transnationally is essential to realizing the full potential of BOT, to expose networks of IFFs and support robust and efficient due diligence in the global economy.

e-Filing

Globally, a large number of countries have adopted asset and interest disclosure systems for public officials to prevent conflicts of interest and promote integrity. These systems vary in scope and filer requirements, with a growing trend towards electronic filing (e-filing).³⁸ e-filing for asset and interest disclosure offers four key benefits: it simplifies the process for those declaring, enhances data management and security, improves the effectiveness of review and enforcement processes, and boosts transparency and public accountability. While it poses initial challenges like costs and training needs, the transition to electronic systems offers significant benefits, including improved compliance and public transparency. Countries worldwide, with diverse internet and technology capacities, have successfully implemented these systems.

33 Open Ownership (2021), <http://standard.openownership.org/en/latest/examples/index.html>, accessed 21 January 2021.

34 <https://datareview.openownership.org>.

35 <https://standard.openownership.org/en/latest/schema/schema-browser.html>.

36 <https://standard.openownership.org/en/0.2.0/schema/reference.html>.

37 <https://standard.openownership.org/en/latest/schema/guidance/>.

38 Kotlyar, D, and L. Pop. (2019). E-filing Asset Declarations: Benefits and Challenges. World Bank, Washington, DC. <http://hdl.handle.net/10986/32066> License: CC BY 3.0 IGO, accessed 21 January 2021.

There is an urgent need to implement electronic systems for uploading and storing data centrally, ensuring data preservation and facilitating its further analysis and processing. Equally important is the capability to capture and process data in a format that not only allows for future publication but also ensures it is machine-readable for reuse.

e-filing systems for asset declarations offer several key features. Firstly, they incorporate validation mechanisms to prevent errors, minimize inaccuracies, and enhance data quality. These mechanisms may include real-time validation of data entry through comparisons with external registries. Secondly, these systems are adaptable, allowing for easy adjustments to the declaration form to accommodate legal changes and enhance user experience. Thirdly, they ensure data integrity and security through processes such as electronic document signing with digital signatures and the implementation of procedures to protect personal data within declarations. Lastly, electronic systems provide a user-friendly interface, streamlining the submission process, reducing errors, and promoting compliance with submission requirements while fostering improved accountability and transparency through enhanced data disclosure to the public.

OECD (2023) suggests the use of electronic submission systems with non-ambiguous data requests, clear and readable information, and pull-down menus to facilitate the verification process. Moreover, the electronic submission system would allow for an effective automated risk analysis, which would depend on external factors such as access to external sources of information through automated data exchange. The system would also help raise the level of compliance with submission requirements and facilitate further analysis and verification of declarations. Additionally, OECD (2023) recommends the development of a risk-based methodology for the review of submissions, which would benefit from clear and standardized data to effectively assess declarations.

Digital declaration systems can track compliance automatically, send reminders or trigger sanctions for non-compliance, and detect breaches to integrity by flagging inconsistencies and anticipating conflicts of interest. They can also be used to publish data and foster public trust, while protecting public officials' private data through various safety measures such as data integrity, data security, and data protection. In order to obtain higher compliance rates and better quality data, strategies such as standardization and the use of artificial intelligence should also be used with the digital declaration systems.³⁹

The e-Register of Asset Declarations in Ukraine, launched in 2016, is a ground-breaking digital system aimed at reducing corruption by mandating public officials to disclose their assets and earnings. This innovative platform is characterized by its automated data collection and analysis, encompassing both asset management and conflict of interest issues. It efficiently performs automatic data verification and is integrated with multiple state registers to manage over a million declarations each year. Developed using a mix of open source and proprietary software, the system is designed for flexibility and ongoing improvements. The initiative has significantly enhanced transparency in public institutions, gaining widespread attention and use, evidenced by the creation of over 7 million documents. However, it faced challenges such as the need for

³⁹ Network for Integrity (2020). Developing digital tools to promote transparency in public life. Article published on 14 December 2020. Available at <https://networkforintegrity.org/the-news/>, accessed 21 January 2021.

rapid development and handling technical demands during high activity periods. Its effectiveness is rooted in a solid legislative framework coupled with adept technical implementation, making it a potential model for replication in other countries. The project underscores the importance of technical adaptability and sensitivity to the political context for successful deployment.⁴⁰

Data sources

BO and PEP transparency are a critical component of the global fight against financial crimes. While countries have varying approaches to defining BO or different thresholds, it is important to review BOT in the global context. Combining BO data with the widest possible range of financial and personal information can provide a more comprehensive and accurate picture of BO.

In addition to traditional information sources, it is helpful to piece together all the information from new and non-traditional sources. The verification of BO information requires other sources of data to corroborate the information. For example, the address should be tested against geographical spatial data to ensure that it is a real address instead of a forest or an abandoned place without infrastructure. For investigative purposes, the address should even be within the person's activity range traced by GPS. For public officials' asset declaration, one can use external sources such as media reports, comparison of declarations over time, and cross-checking with other government databases as part of the risk analysis framework.

Non-traditional data sources can also be used to verify BO information. These sources include geospatial data, such as drones, sensors, remote sensing, meters, and POS scanners. Image data, such as tollbooth cameras and security cameras, can also be used to verify BO information. Personal information, such as mobile phones, financial records, social media, and newsletter subscriptions, can provide additional data points to corroborate BO information. Commercial data, such as supermarket scanners, Google searches, Uber, Amazon, and Yelp, can also be used to verify BO information. Business data, such as job postings, employment history, and utility bills, can also provide useful information to corroborate BO information. Open-Source Intelligence (OSINT) encompasses publicly available information from a variety of online and offline sources, including social media, news articles, public records, and academic publications. Analysing OSINT can provide valuable insights into criminal networks, illicit activities, and emerging trends. Analysing mobile phone records and communication data can provide insights into the networks and interactions of criminal groups, as well as aid in identifying key individuals involved in illicit activities. Data related to public health, such as patterns of substance abuse, overdose incidents, and disease outbreaks, can provide indicators of organized crime involvement in drug trafficking and other illicit activities. Leveraging non-traditional data sources for social network analysis can help identify connections and relationships within criminal networks, uncovering hidden associations and facilitating targeted investigations.⁴¹

⁴⁰ <https://oecd-opsi.org/innovations/e-register-of-asset-declarations-of-public-officials-in-ukraine/>, accessed 21 January 2021.

⁴¹ Op. cit., UNODC (2021).

For example, some tax authorities, FIUs and LEAs now use data mining, artificial intelligence, and deep learning to cross-analyse data they already have with data from external sources, including that derived from the automatic exchange of tax information and social media.⁴²

By combining traditional and non-traditional data sources, governments can enhance the accuracy and completeness of BO information. This can help to identify and prevent financial crimes, promote transparency, and ensure a more secure and stable financial system. However, it is important to ensure that the collection and use of data is done in a responsible and ethical manner, with appropriate safeguards in place to protect individual privacy and data security.

Data interoperability

Interoperability refers to the ability of different systems, technologies, and databases to work together seamlessly and effectively. It is essential for enabling the exchange of information between different government agencies.

To effectively combat corruption, ML and TF, and illicit activities, there is a need for a uniform data standard that can be applied across different institutions and borders. Adopting a common data schema, like the BODS framed by JSON Schema 0.4, promotes data interoperability, facilitating the smooth exchange of information among various entities. Adopting standardized data formats and protocols ensures that data can be easily exchanged and understood across different systems and platforms. This promotes consistency and compatibility, reducing barriers to data sharing and analysis.

The integration of clear identifiers such as company registration and individual taxpayer numbers is crucial. These identifiers enable accurate matches in disclosures, distinguish entities with similar information, and reduce the incidence of both false positives and negatives, thereby improving the reliability of BO data.

The implementation of automatic and real-time data exchange protocols is crucial for matching information precisely, enhancing the interoperability of data among public and private institutions. Such a system improves the efficacy of investigations and bolsters the transparency and integrity of BO information. Thus, interoperable data systems enable real-time access to critical information, allowing law enforcement and regulatory agencies to respond swiftly to emerging threats, track IFFs, and identify high-risk individuals or entities involved in criminal activities.

Furthermore, agencies require sophisticated tools for identifying and tracing connections within the data collected. These tools should enable the linking and analytical examination of databases, such as through data analytics. Policymakers can advance this cause by mandating the interlinking of agency databases, allowing for the triangulation of collected data.

⁴² Op. cit., Brun, et al. (2022).

The deployment of advanced technologies, like artificial intelligence (AI) and neural networks, can significantly aid in triangulating data from diverse sources, including company registries, tax records, land registries, and other financial documents. This technology-driven approach can significantly enhance the ability of agencies to trace and analyse complex information webs, crucial for effective regulatory oversight and enforcement.

Information exchange

The fight against financial crimes, including tax evasion, ML, and corruption, requires a whole-of-government approach that emphasizes cooperation and information sharing among various agencies. This approach involves breaking down silos and fostering integrated inter-agency collaboration to bolster investigations and prosecutions of financial crimes. By dismantling barriers that impede cooperation and information sharing, countries can create a more complete picture of financial crimes, generate more actionable and accurate information, and ultimately achieve greater efficiency in carrying out their respective mandates.

For information exchange, developing internal standard operating procedures governing the inter-agency exchange of information, specifying the nature of information to be shared, the time frame, and the exact steps to follow is crucial for effective collaboration.⁴³ Technical and structural elements must be in place to ensure that information flows smoothly in a timely, cost-efficient way. This includes designing and implementing effective internal policies and procedures governing inter-agency cooperation and developing the technological capabilities needed to share sensitive and potentially large volumes of data while securing the confidentiality of the information.

There is also a need to establish a fluid, secure system for exchanging information.⁴⁴ A legal framework that provides the policy tools for and legitimizes effective inter-agency cooperation should be supplemented by procedures to operationalize such exchanges within and among agencies. Beyond mapping out the responsibilities of each agency and method of information sharing, countries should assess the security of information-sharing platforms, their confidentiality, and their compliance with data protection requirements.

National frameworks must ensure the security, confidentiality, and data protection compliance of information-sharing platforms. A robust system of financial intelligence sharing might utilize cloud servers for data availability, with stringent privacy and security measures in place. In the investigative phase, databases often become more extensive, as tax authorities, FIUs, and LEAs need comprehensive data to pursue leads. These agencies can share information through established legal frameworks and protocols.

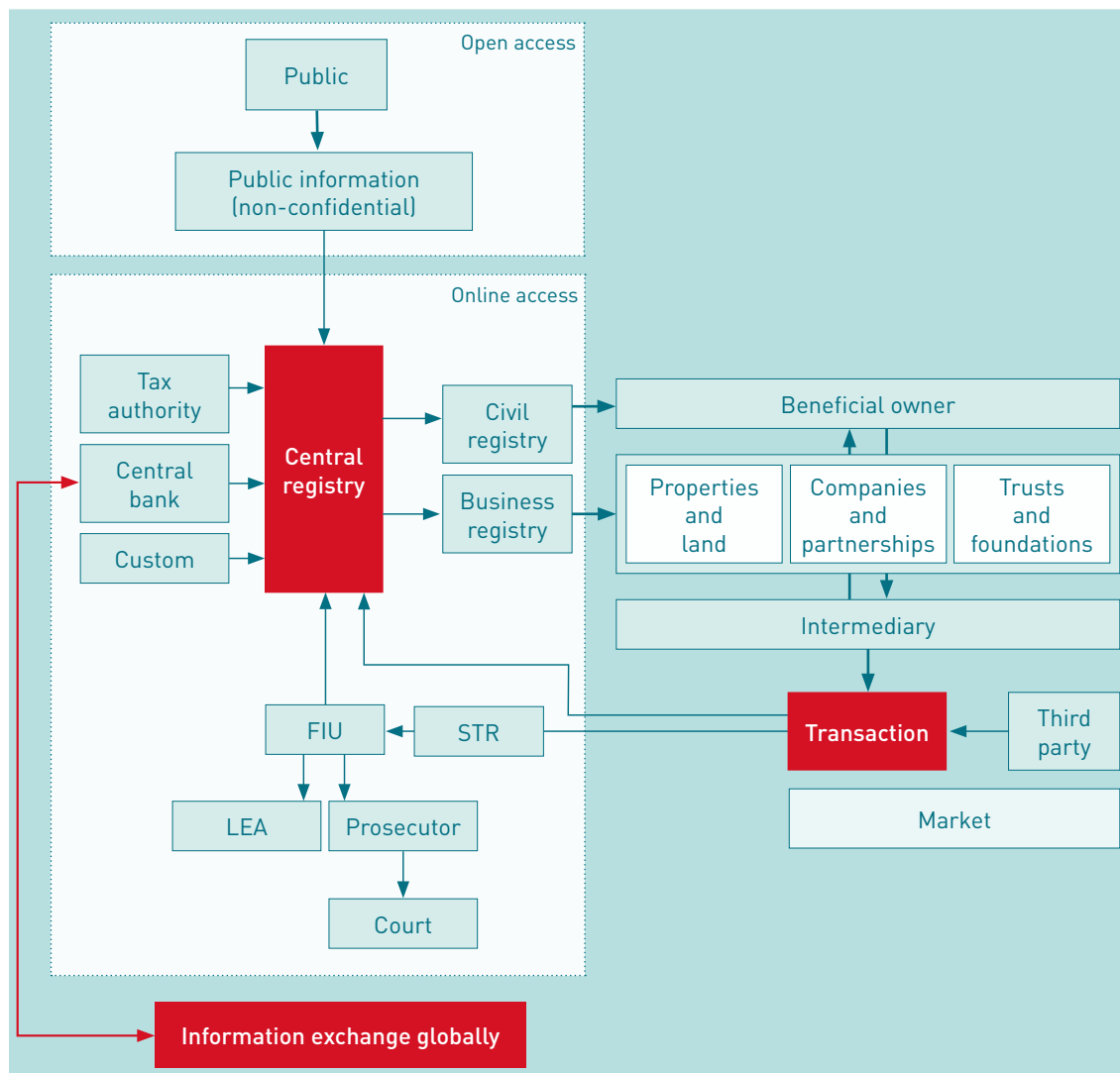
⁴³ Ibid.

⁴⁴ Ibid.

Registries

Maintaining a central register of BO is one of the three complementary approaches identified by the FATF as a global best practice. The FATF has identified central registers as a crucial tool for reducing ML risk, and countries that maintain a central register perform better against FATF’s requirement to ensure timely access to adequate, accurate, and up-to-date information on the BO of companies.⁴⁵

Figure 6: A BO central registry with numerous third-party data interfaces



The FATF guidance recommends that the following information should be collected to identify and verify the natural person(s) who are the beneficial owner(s) of a legal person: the first and last name of the beneficial owner(s), their nationality(ies), date of birth, a unique national identification number such as an internal administration number, a tax registration number, an identity number, or a social security number, passport number and document type, place of birth, residential address, and the tax identification number or equivalent in the country of residence of the beneficial owner(s). This list is not exhaustive, and countries may consider

45 Op. cit., FATF (2023b)

recording additional information to further confirm the identity of the beneficial owner(s). However, the guidance emphasizes that the information collected should be adequate, accurate, and up-to-date to ensure the effective identification and verification of BO.⁴⁶

A centralized BO register allows authorities and designated users to access information on the BO of companies and PEPs through one central location in a standardized format. This is a key requirement for an effective BO register that allows data to be used by all user groups while removing the time and cost implications of having to access, reformat, clean, match, and analyse the information.

Making the BO register accessible to the public means that LEAs, businesses, journalists, and citizens from around the world can easily access the BO information of companies, subject to relevant privacy laws. Having widespread third-party data improves data quality by increasing the user base beyond authorities. Publicly available BO data can reduce the cost and complexity of due diligence and risk management for the private sector, thereby levelling the playing field and increasing competitiveness. Evidence shows that data in a public register is used much more widely when it is freely available and open. This is critical for analysing BO across multiple jurisdictions when tracing the transnational links between companies.

Disclosure and publication of BO information have legitimate public interest purposes and can be compliant with data protection and privacy legislation. The fields of data that are collected and published, including identifiers, should be developed in the context of local legislation while maximizing the availability of information that supports effective data use. Similarly, the disclosure requirements should cover all classes of natural persons, including domestic and foreign citizens who meet the definition of beneficial owner and PEPs, to close loopholes that could be exploited to avoid disclosing ownership.

Open data is one of the best ways to publish BO information while still ensuring that personal information is secure and private. Strong security features should be associated with a central register, while providing the widest possible range of people and organizations that can access it, therefore driving the AML/CFT and anti-corruption policy impact.

It is recommended that countries have a central registry that follows the FATF's multi-pronged approach, which encompasses a registry, companies, and existing information approach and includes a combination of tiered and public access. Law enforcement and similar authorities and other designated users should have full authorized access to all the information in the register, while the public has access to legal entity and less sensitive information, ensuring that individuals' personal information is protected and that they are not vulnerable to cybercrime in the form of identity theft.

In addition to maintaining a central register of BO, countries should also ensure that trustees or persons holding equivalent positions in similar legal arrangements are not prevented by law or enforceable means from providing financial institutions and DNFBPs, upon request, with

⁴⁶ Ibid.

information on the BO and the assets of the trust or legal arrangement to be held or managed under the terms of the business relationship.

To determine who the beneficial owners of a company are, competent authorities require certain basic information about the company, which, at a minimum, would include information about the legal ownership and control structure of the company. All companies created in a country should be registered in a company registry, and the minimum basic information to be obtained and recorded by a company should include the company name, proof of incorporation, legal form and status, the address of the registered office, basic regulating powers, a list of directors, and a unique identifier such as a tax identification number or equivalent.

Transparency and BO of legal persons and arrangements are crucial in assessing the risks of misuse of legal persons for ML or TF. Countries should ensure that there is adequate, accurate, and up-to-date information on the BO and control of legal persons that can be accessed rapidly and efficiently by competent authorities, through a register of BO or an alternative mechanism. Countries should also take effective measures to ensure that nominee shareholders and directors are not misused for financial crime.

Countries should consider complementary measures as necessary to support the accuracy of BO information, such as discrepancy reporting. Competent authorities, and in particular LEAs and FIUs, should have all the powers necessary to be able to obtain timely access to the basic and BO information held by the relevant parties, including rapid and efficient access to information held or obtained by a public authority or body or other competent authority on BO information or on the financial institutions or DNFBPs which hold this information.

It is important to note that the FATF recommendations are regularly updated to reflect changes in the global landscape of ML and TF. Countries should stay apprised of the latest recommendations and guidance documents published by the FATF to ensure that their AML/CFT policies and practices are effective and compliant with international standards.

For asset declaration of PEPs, it is recommended to establish a central asset registration systems and databases throughout the asset management process, emphasizing the need for information technology systems and databases for asset registration. It is also important to use appropriate financial and property administration IT systems for tracking and managing inventory, meeting expenses associated with seized property, and maintaining a transparent and accountable system.

A centralized database is a type of database system in which all data is stored in a single location. In the context of asset recovery, a centralized database or system is used to record and track assets, including financial holdings, real estate properties, vehicles, and other valuable possessions. This database or system serves as a central repository of information, allowing for efficient tracking and management of assets. It may be accessed by authorized personnel, such as LEAs, FIs, and other relevant stakeholders, to facilitate the recovery of assets that have been acquired through illegal means or are subject to forfeiture. The use of such a system can help to improve transparency, accountability, and efficiency in asset recovery efforts.

It could also potentially support the implementation of direct enforcement mechanisms for foreign restraint and confiscation orders. If this system could serve as a centralized repository for information related to restrained and confiscated assets, it could streamline the process of tracking and managing these assets, thereby contributing to the effectiveness of international cooperation in asset recovery.

The use of a centralized database aligns with the broader recommendations for jurisdictions to develop specialized knowledge about the direct enforcement of foreign confiscation orders within competent authorities, as well as to enhance cooperation and coordination among relevant stakeholders involved in asset recovery efforts. Therefore, the implementation of a centralized database or system could be a valuable component of a comprehensive approach to improving the decision framework for direct enforcement of foreign restraint and confiscation orders.⁴⁷

Key recommendations from FATF include:⁴⁸

- **Filing BO information:** Legal persons, such as firms and companies, are required to obtain and hold adequate, accurate, and up-to-date BO information. This information typically includes details about the natural person(s) who are the beneficial owner(s), such as their full name, nationality, date and place of birth, residential address, national identification number, and tax identification number. Trustees of express trusts and persons holding equivalent positions in similar legal arrangements are required to obtain and hold adequate, accurate, and up-to-date BO information regarding the trust and other similar legal arrangements. This includes information on the settlor(s), trustee(s), protectors (if any), beneficiaries, and any other natural person(s) exercising ultimate effective control over the trust.
- **Access to BO information:** Competent authorities, particularly LEAs and FIUs, should have the necessary powers to obtain timely access to the basic and BO information held by relevant parties, including rapid and efficient access to information held or obtained by public authorities or other competent authorities on basic and BO information. This access is essential for conducting investigations and ensuring transparency in BO. DNFBPs should have mechanisms to ensure timely access to BO information of legal persons, including firms and trusts. This access is crucial for conducting due diligence, investigations, and overall efforts to combat ML and TF.
- **Up-to-date information:** Countries should ensure that BO information is as current as possible and is updated within a reasonable period following any change in order to maintain its accuracy and reliability.
- **Company registry access:** Countries should require their company registry to facilitate timely access by financial institutions, DNFBPs, and other countries' competent authorities to the public information they hold, including BO information, for reasons of due diligence and transparency.
- **Transparency of BO:** Countries should consider facilitating public access to BO information held by company registries. This transparency can contribute to the overall

47 Betti, S., Kozin, V. and J-P. Brun (2022). *Orders without Borders: Direct Enforcement of Foreign Restraint and Confiscation Decisions*. StAR, World Bank Group. Available at https://star.worldbank.org/sites/default/files/2021-12/Orders%20without%20Borders_final.pdf.

48 Op. cit., FATF (2023b).

efforts to combat ML and TF by promoting accountability and deterring illicit activities. Countries should consider complementary measures, such as discrepancy reporting, to support the accuracy of BO information. Additionally, legal persons and entities involved in maintaining BO information should maintain the information and records for a specified period, typically at least five years after the company ceases to exist or ceases to be a customer of the professional intermediary or financial institution.

In the context of PEPs, the following is recommended:⁴⁹

- **Risk assessment:** FIs should conduct a risk assessment to determine whether a customer or beneficial owner is a PEP. This assessment should take into account the nature of the customer's business, the customer's country of origin, and the customer's position or relationship with a government or international organization.
- **Enhanced due diligence:** FIs should apply enhanced due diligence measures for PEPs, including obtaining senior management approval for establishing or continuing business relationships with PEPs, taking reasonable measures to establish the source of wealth and source of funds, and conducting enhanced ongoing monitoring of the business relationship.
- **Family members and close associates:** The requirements for all types of PEPs should also apply to family members or close associates of such PEPs. FIs should apply enhanced due diligence measures for these individuals as well.
- **Domestic PEPs:** FIs should take reasonable measures to determine whether a customer or beneficial owner is a domestic PEP or a person who is, or has been, entrusted with a prominent function by an international organization. In cases of a higher risk business relationship with such persons, FIs should apply the measures mentioned above.

Digital ID as a means of verifying beneficial owners and PEPs in the registry

Information about the beneficial owner needs to be verified at the point of being onboarded in the central registry. Digital identity can be used to verify and even authenticate a natural person or beneficial owner of an entity, resulting in the successful linking of legal entities and arrangements to the natural person. The collection of verified identity attributes including passports, national ID, driver's licenses, biographic and biometric data can facilitate increased accuracy and better compliance. "Digital ID systems that meet high technology, organizational and governance standards hold great promise for improving the trustworthiness, security, privacy and convenience of identifying natural persons in a wide variety of settings, such as financial services, health, and e-government in the global economy of the digital age. These digital IDs are referred to as those with higher assurance levels."⁵⁰

The key to a robust and effective BO and PEP transparency disclosure solution depends on the following (illustrated in figure 7):

49 Ibid.

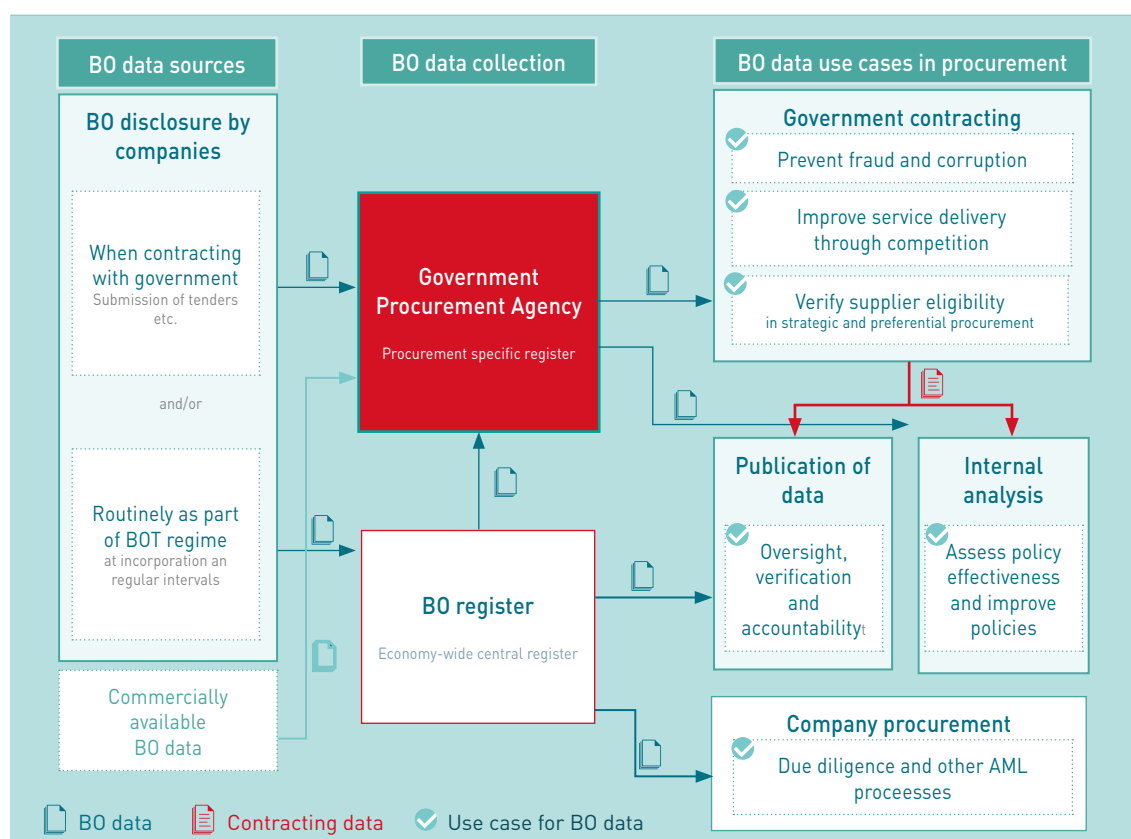
50 FATF (2020), Guidance on Digital Identity, FATF, Paris, www.fatf-gafi.org/publications/documents/digital-identity-guidance.html

- **Strengthening the collection of BO information:** improving disclosure requirements of different types of various legal vehicles is fundamental to improving transparency.⁵¹
- **Improving the interoperability of information:** the use of one standard, such as BODS, will improve data sharing and cross-border collaboration.
- **Building strong verification systems:** Improving business verification methods helps ensure accurate and usable data.
- **Engaging citizens in monitoring and accountability:** creating channels for feedback and information broadens the oversight to help discover webs of corruption.

BO and public procurement

BOT in public procurement plays a pivotal role in safeguarding the integrity of the process by preventing corruption and fraud.⁵² Leveraging BO data enables the detection of individuals or entities attempting to manipulate legislation and contracting procedures for personal gain. This transparency also enhances due diligence, allowing for the identification and deterrence of fraudulent activities within the procurement ecosystem. Moreover, by revealing the authentic ownership structure of companies, BO data assists in uncovering potential conflicts of interest and IFFs, thereby promoting transparency and accountability.

Figure 7: BO and public procurement



51 For further information, see: <https://www.openownership.org/en/publications/beneficial-ownership-declaration-forms-guide-for-regulators-and-designers/>.

52 Open Ownership (2021). *Beneficial ownership data in procurement*. Available at <https://oo.cdn.ngo/media/documents/oo-briefing-bo-data-in-procurement-2021-03.pdf>.

Operationalizing the use of BO data in procurement involves a multifaceted approach. It necessitates the sourcing of reliable and comprehensive registers or datasets, ensuring the accuracy and completeness of the information. The collection, verification, and publication of this data in a format that allows for seamless linkage to other datasets is crucial for its effective utilization. Also, employing advanced data collection methods and verification processes is essential to maintain the quality and usability of the data, for informed decision-making.

Structured and interoperable BO and procurement data offer a myriad of potential benefits for public access. By enabling public oversight and accountability, this data empowers stakeholders to verify and conduct due diligence processes effectively, thereby enhancing transparency and trust in the procurement process. It allows for comprehensive policy analysis, enabling governments to assess the effectiveness of procurement policies and make informed decisions for future policy development. Additionally, it provides a valuable reference dataset for procurement agencies, potentially offering higher quality data for in-depth analysis and strategic decision-making.

To implement BOT in public procurement, a clear legal framework defining BO and setting low thresholds for disclosure should be established. This framework should comprehensively cover all relevant types of legal entities and natural persons. Governments can collect BO data during the procurement process and hold it in a central procurement-specific register or pull data from a central BO register that covers all sectors of the economy into procurement processes. Measures should be taken to verify the BO data to ensure its accuracy and reliability, including implementing processes for ongoing verification and updating of the data.

Making the BO data accessible to the public in a structured and interoperable format is crucial, as it promotes public oversight and accountability. Collaboration with relevant stakeholders, including procurement authorities, civil society, and private sector actors, is also important to ensure effective implementation and utilization of BO data in public procurement. Aligning the implementation with international standards and best practices, such as the Open Ownership Principles, is recommended to ensure high-quality, reliable data that maximizes usability and minimizes loopholes. Additionally, providing training and capacity building for government officials and stakeholders involved in the collection, verification, and use of BO data in public procurement is essential. Establishing mechanisms for monitoring compliance with BO disclosure requirements and enforcing sanctions for noncompliance is a critical aspect of successful implementation.

FATF recommended that countries must guarantee that public authorities at the national level and other relevant entities have prompt access to fundamental and BO details concerning legal entities during public procurement. They should employ a RBA to ascertain the necessary level of access to BO information for public procurement processes, considering the ML and TF risks associated with the procurement process and the involved legal entities. Moreover, countries should mandate that legal entities participating in public procurement processes furnish sufficient, precise, and current BO information. This information should be promptly accessible to competent authorities and other pertinent parties.⁵³

⁵³ Op. cit., FATF (2023b).

Use of new technologies

KYC utilities

KYC utilities play a pivotal role as centralized platforms for managing CDD information, enabling the sharing of AML/CFT compliance costs among banks. These utilities are designed to collect, verify, and securely store essential data for customer identification and due diligence. Member financial institutions can leverage the data housed within these utilities to streamline their own KYC processes. Ownership structures and target markets of these utilities can vary, with some focusing on scrutinizing PEPs while others may have a different emphasis.

A notable advancement in this realm is the emergence of the BODS developed by Open Ownership. This standard establishes a unified framework for BO utilities, with a focus on ensuring the integrity of data, interoperability, customization, and the propagation of best practices.

The adoption of these utilities offers numerous advantages. By leveraging existing KYC infrastructure and governance frameworks, FIs can benefit from cost reductions through economies of scale. This approach minimizes redundant efforts in gathering beneficial owner information, ultimately leading to decreased overall expenses. Moreover, these utilities have the potential to provide coverage across multiple jurisdictions and can serve as a means to pool resources from both public and private entities, further driving down costs associated with CDD, Enhanced Customer Due Diligence (ECDD), KYC, and PEP scrutiny.

However, there are challenges and potential drawbacks. Some utilities may not be freely accessible, and certain ones might not encompass PEP analysis or the aggregation of digital identity information, which are critical components for their effectiveness. The need for specialized governance structures to oversee data trusts and the variance in data analysis methodologies could introduce complexity. Furthermore, the proliferation of multiple utilities could diminish the benefits of economies of scale, and a singular utility could raise concerns related to monopolistic practices unless it operates as an open, public register. Additionally, the sharing of information across jurisdictions could be hindered due to data privacy regulations.

A recommended course of action could be the establishment of a structured, machine-readable Beneficial Ownership Data Trust that integrates KYC utilities into a comprehensive, multi-jurisdictional system. This approach has the potential to yield cost savings for both public and private sector institutions, enabling them to allocate resources away from non-revenue-generating activities that are essential for compliance. The initiatives undertaken by Open Ownership serve as a prominent model in this domain.

Three distinct models have emerged for such a utility, each offering different benefits based on the legal operating model adopted by banks:⁵⁴

⁵⁴ <https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/a-kyc-aml-utility-driving-scale-efficiency-and-effectiveness>

- **Model 1:** A static KYC-AML data repository involves the collection and sharing of information among member banks. This repository includes static KYC data such as beneficial owners for corporate entities and up-to-date KYC information for retail customers. AML-related data may comprise customer blacklists, whitelists of reviewed and trusted customers, PEP status, sanctions status, and reports on suspicious activities or transactions (SARs/STRs). Under this model, the utility streamlines onboarding processes by providing a single platform for accessing KYC and AML information for new customers, eliminating the need for repeated requests for such information.
- **Model 2:** A transaction-analysis AML utility consolidates encrypted transaction-level data into an analytical solution, enabling advanced transaction monitoring and screening capabilities across a broader network of transactions. Banks using this model can significantly reduce their AML risk.
- **Model 3:** A fully outsourced AML utility focuses on helping member banks improve AML operations and the efficiency of select AML processes by employing operational units for enhanced due diligence and customer investigations.

All three models offer benefits to banks, which increase alongside the level of information sharing within the system. However, the third model, a fully outsourced utility, may need to be developed incrementally due to the complexity of bank systems and requirements, starting with the development of a data repository or transaction-analysis capabilities.

Social network analyses

A comprehensive and effective BO register, whether publicly accessible or centralized, necessitates a thorough and sophisticated approach to bolster AML/CFT endeavours. However, simply focusing on scrutinizing PEPs and BO is inadequate due to the intricate layering schemes employed by individuals through global conglomerates, characterized by complex networks of cross-ownership, control, and co-investment. Leveraging network graph analytics is invaluable in simplifying the comprehension and tracing of complex transactions by tracking these intricate networks.

Network analysis, a discipline that harnesses big data analytics, AI, network statistics, ML, and fuzzy logic, plays a pivotal role in identifying the ultimate beneficial owner. This methodology involves constructing a network of inter-relationships among individuals, legal entities, and various asset classes, tracing financial transaction linkages, and visualizing a map of interrelationships sourced from diverse data outlets. Fuzzy logic, in particular, enhances the matching of customer identities and fortifies the identification of the ultimate beneficial owner within a BO register.⁵⁵

Governments and financial institutions must leverage these advanced tools and techniques to amalgamate multiple internal and external databases, both domestically and internationally, to enhance screening capacities for evidence of wrongdoing.

55 Fonzetti Colladon, A. and E. Remondi (2017). Using Social Network Analysis to Prevent Money Laundering. *Elsevier Expert Systems with Applications*, vol 67, January 2017, pp. 4–58. Available at <https://doi.org/10.1016/j.eswa.2016.09.029>

Nevertheless, the implementation of these technologies presents its own set of challenges. Developing effective algorithms necessitates skilled experts, as inexperienced programmers may generate an excess of false positives. The process is resource-intensive, requiring substantial hardware or cloud storage. Additionally, maintaining data integrity to prevent it from devolving into a data swamp is costly and labour-intensive. Moreover, the proliferation of network analyses by numerous institutions leads to some duplication of efforts, further escalating costs and inefficiency.

To mitigate these challenges, it is recommended that BO information within a central or public registry be analysed using social network analyses, fuzzy logic, AI, and/or ML. This approach would enhance the matching of individuals and map the inter-relationships between individuals, their legal entities, and assets, thereby bolstering the effectiveness of AML/CFT measures.

Big data analytics, AI and ML

The fight against financial crimes is increasingly powered by advanced technologies such as big data analytics, AI, and ML. These tools are vital in modernizing systems for pooling and analysing data, which simplifies administration and helps agencies link and track various information sources. By integrating data analytics, AI, and deep learning, cross-analysis of diverse data sources becomes feasible, including data from automatic tax information exchanges and social media, aiding in triangulating information from sources like company registries, tax databases, and land registries. This enhancement in capabilities is crucial for tax authorities and law enforcement in investigating and prosecuting financial crimes.

Big data encompasses datasets too large for standard database software to handle in terms of capture, storage, management, and analysis. Characterized by high volume, velocity, and variety, it requires distinct hardware, software, and analytical solutions compared to traditional datasets. This is particularly relevant in the data-intensive financial sector.

AI applications combine several technologies like software, algorithms, big data, cloud computing, and sensory interfaces to mimic human cognitive abilities. There are seven branches of AI, each applying cognitive intelligence to machines in different ways, including ML, natural language processing, speech, expert systems, planning, scheduling, optimizing, robotics, and vision.

Effective supervision and oversight in mitigating ML and TF involve first collecting and storing data in a data lake. This data must then be cleaned, verified, and maintained. Fuzzy logic and ML are often applied to link various datasets, creating comprehensive datasets. Experienced and sophisticated ML techniques are crucial for analysing transactions, linking them to individuals, creating network analyses and graphs, and gathering statistics. ML can enhance several compliance functions, improving customer typologies and monitoring transactions to reduce false alerts and identify illicit finance techniques.

The use of big data, AI, and ML has several advantages. They can analyse large datasets quickly, revealing relationships and patterns that human analysts might miss. This technology is particularly effective in examining PEPs and their connections, reducing the need for extensive

investigative resources. ML excels in identifying nonlinear patterns in big data, and fuzzy logic can help match entity information. These tools simplify AML and fraud detection, save time and money for governments and financial institutions, and contribute to reducing fraud, corruption, ML, and tax evasion. Big data applications offer lower storage costs and faster refresh rates, allowing for the use of larger, more comprehensive datasets in AML/CFT monitoring.

However, challenges include the need for skilled experts to design, build, and train AI and ML models. Poor data quality can impede AI and ML models, and regulatory restrictions on data usage may limit their effectiveness. The technology is resource-intensive, requiring substantial storage capacity, and maintaining data integrity is costly. The development of network analyses by multiple institutions leads to duplicative efforts, increasing costs and inefficiencies. Moreover, data protection laws can hinder data sharing.

The recommendation, therefore, is to employ AI and ML to consolidate large datasets from various sources. Analysing these datasets to scrutinize PEPs and beneficial owners, while continuously verifying, updating, and maintaining them, can create the financial intelligence necessary to combat IFFs, corruption, tax evasion, ML, TF, and proliferation financing. These technologies also enable the analysis of transactions and their connection to individuals, creating network analyses and statistics. ML enhances compliance functions, developing sophisticated customer typologies and improving transaction monitoring. This leads to fewer false alerts and the identification of illicit financial activities.

Digital identification, biometrics and self-sovereign identification or digital identity wallets

Digital identity is a crucial aspect of the digital age, as it can link a real entity, such as a natural person, to its digital equivalent entities. The collection of verified identity attributes, including passports, national ID, driver's licenses, biographic and biometric data, can facilitate increased accuracy and better compliance. "Digital ID systems that meet high technology, organizational and governance standards hold great promise for improving the trustworthiness, security, privacy and convenience of identifying natural persons in a wide variety of settings, such as financial services, health, and e-government in the global economy of the digital age. These digital IDs are referred to as those with higher assurance levels."⁵⁶

In the fight against financial crimes, digital identification, biometrics, and self-sovereign identification can provide a more secure and accurate BO register. Digital identity systems have the potential to revolutionize the way we identify individuals in various settings, including financial services, health, and e-government.

Digital identity is a collection of electronically stored attributes and credentials that uniquely identify a person, while digital identification is the process of validating a person's attributes to establish their digital identity. Identity attributes are discrete pieces of information attached

⁵⁶ FATF (2020). *Guidance on Digital Identity*. FATF, Paris. Available at www.fatf-gafi.org/publications/documents/digital-identity-guidance.html.

to a person's or entity's identity.⁵⁷ Biometrics, such as automated biometric recognition using fingerprints or iris scans, ensure unique identities and provide a convenient, password-free authentication method. Biometrics serve three functions: identification (determining who someone is), authentication (confirming claimed identity), and authorization (establishing rights in a system).

Multi-layered or multi-factor authentication, which combines biometrics with other credentials, enhances the accuracy and security of biometric systems. In addition to physical biometric traits, AI and ML can use certain unalterable traits of human characteristics, such as behavioural patterns, as unique identifiers. This can further enhance the accuracy and security of digital identity systems.

Self-sovereign identity (SSI) gives individuals full control of their identifiers and the data associated with them, allowing them to control who they share their data with. This can include verifiable credentials obtained from a single verifiable golden source (i.e. an identity document, passport) or less other sources including, social media account information, and attestations from friends and colleagues. In a decentralized digital identity world, anyone can issue a credential or perform an attestation for someone else, but there are different levels of trustworthiness. SSI allows individuals to control who has access to their information, based on when they engage with different institutions, without contravening any data privacy issues. This can create a more secure and accurate BO register.

While centralized identity management facilitates the tracking of data, SSI leverages user information in diverse, unrelated patterns, bolstering privacy. The three fundamental components of SSI actively contribute to the establishment of digital identities and credentials that are impervious to fraud. SSI's distinctive technology ensures the security and integrity of credentials without dependence on centralized storage. Furthermore, validation of the owner's real-world identity becomes straightforward using blockchain-powered Uniform Resource Identifiers (URIs), also known as Decentralized Identifiers (DIDs). These three pillars – Decentralized Identifiers (DIDs), Verifiable Credentials (VCs), and Blockchain – constitute the cornerstone of SSI.⁵⁸

To make a decentralized SSI identity system work, certain capabilities need to be in place, including the ability to issue and verify credentials, the ability to store and manage identity data, and the ability to establish trust between different parties. It is important to ensure that these systems meet high technology, organizational, and governance standards to ensure their trustworthiness, security, privacy, and convenience.

Digital identity systems have the potential to revolutionize the way we identify individuals in various settings, but it is important to ensure that these systems meet high standards to ensure their trustworthiness, security, privacy, and convenience.

57 World Bank (2016). Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation. A Joint World Bank Group – GSMA – Secure Identity Alliance Discussion Paper. Available at <http://documents1.worldbank.org/curated/en/600821469220400272/pdf/107201-WP-PUBLIC-WB-GSMA-SIADigitalIdentity-WEB.pdf>, accessed 17 December 2020.

58 <https://www.identity.com/self-sovereign-identity/>.

DLT and blockchain

Blockchain technology has emerged as a revolutionary system for synchronized digital databases replicated across a network of computers. It enables the secure storage, sharing, and transfer of information without needing a central administrator. DLT operates on peer-to-peer networks without a central hub, contrasting with traditional databases that rely on a central server for validation and control. In DLT, all nodes share the responsibility of managing the database, functioning as both clients and servers. The unique aspect of blockchain is its data structure. Data updates, agreed upon by the majority of network nodes, are batched into a block, time-stamped, and cryptographically linked to the preceding block, forming a chain. This results in a continuously updated public ledger across the entire network, with every node maintaining a complete record of all transactions.

Blockchain's applications are varied, with many countries exploring its use in government services. Its advantages include secure registration and storage of information, real-time information sharing, and the facilitation of transactions with transparency, privacy, security, auditability, and immutability. Additionally, it is a resilient technology that enables secure disintermediation and structured, machine-readable data sharing, all with low transaction costs.

However, challenges exist. Scalability and interoperability require collaboration on data standards, and centralized databases can offer similar benefits. Closed, permissioned ledgers with fewer nodes are more vulnerable to security breaches, making permission-less ledgers with proof-of-work consensus more secure. While transactions on the public ledger are pseudo-private, linking them to individuals requires sophisticated intelligence. Governance in peer-to-peer DLT arrangements poses a challenge, and transitioning to new technologies is costly.

The recommendation is to consider DLT and blockchain as platforms for PEP and BO registers. These platforms offer a cost-effective way to store digital identification, BO, and asset information securely and transparently. To enhance these platforms, focus should be on data interoperability standards, like the BODS standard by Open Ownership. Banks moving towards SSI through e-KYC are well-positioned to guide this standard. Furthermore, these platforms should not only serve as compliance tools but also provide benefits to users, allowing them to register and store information about BO and assets like share certificates, facilitating transactions and transfers through the platform. Blockchain technology and DLT present a promising opportunity to address the challenges associated with traditional databases. By embracing these technologies and focusing on enhancing their capabilities, governments and organizations can establish secure, transparent, and cost-effective platforms for managing BO and asset information. Collaboration on data standards and governance will be key to realizing the full potential of these platforms.

The World Customs Organization (WCO) has acknowledged the transformative potential of blockchain technology in enhancing trade facilitation and has embarked on various initiatives to explore its applications. One notable example involves the WCO collaborating with the International Chamber of Commerce (ICC) to develop a blockchain-based solution for the exchange of electronic certificates of origin (eCOs). This innovative solution aims to simplify and streamline the authentication process for eCOs, thereby cutting down the time and expenses

associated with manual verification procedures.⁵⁹ Additionally, the WCO has ventured into the use of blockchain technology in supply chain management, with a specific focus on customs clearance. Leveraging blockchain to establish a secure and transparent digital ledger of all supply chain transactions, customs authorities can effectively monitor the movement of goods and verify their origins, thus mitigating the risks associated with fraud and smuggling. Furthermore, the WCO has identified the potential of blockchain technology to enhance the security and transparency of trade finance. By employing blockchain to create a secure and transparent digital record of all trade finance transactions, banks and financial institutions can easily authenticate trade documents, significantly reducing the likelihood of fraudulent activities.

Existing identifiers for entities including the LEI, the TIN and the EORI numbers of registers

The Legal Entity Identifier (LEI) was introduced as a standardized identification system for legal entities in the aftermath of the financial crisis. This unique 20-character alpha-numeric code is assigned to legal entities, enabling them to engage in transactions and contracts. The primary purpose of the LEI is to uniquely identify parties involved in financial transactions, thereby enhancing financial transparency. Often likened to a legal entity's barcode, the LEI is applicable to a wide range of institutions, including financial and non-financial entities, investment funds, and government agencies. It is characterized by its uniqueness, permanence, neutrality, scalability, reliability, interoperability, transparency, and public availability. The LEI contains a standardized set of information in the Common Data File format, including entity details and information on the ultimate parent of the issuing organization. This standardized information makes it easier for governments and financial institutions to assess the financial risks associated with these entities.

In parallel, the WCO has established guidelines for the Trader Identification Number (TIN), providing standards for creating a globally unique TIN for the exchange of Authorized Economic Operator (AEO) master data. These guidelines facilitate the implementation of AEO-Mutual Recognition Arrangements/Agreements in a standardized manner, thereby avoiding costly fragmentation in the trade space. A common identification number for cross-border trade enhances efficiency for economic operators and customs authorities, improving security, facilitating trade statistics collection, assisting in consignment tracking and tracing, and simplifying information exchange between customs and other government authorities.

Both LEIs and TINs offer several advantages. The LEI complies with the open data charter and is interoperable with other AML/CFT applications, serving as a common reference point. It is distinct and unambiguous compared to the Business Identifier Code (BIC), undergoing strict data validation and reliably identifying parties in payment chains. This reduces uncertainties and processing times, lowers transaction costs, and facilitates automation between institutions and platforms. TINs enhance real-time information sharing between government institutions and customs authorities.

⁵⁹ UNCTAD (2023). *Economic Development in Africa Report 2023*. Available at <https://unctad.org/publication/economic-development-africa-report-2023>.

However, they cannot substitute for due diligence requirements and cannot directly identify natural persons in payment chains. While they assist in identifying legal entities, they do not directly help with BO, requiring complementary personal information. Adoption among non-financial corporations is slow and integrating LEIs into payment systems may be costly and require new technical capabilities.

The recommendation is to use LEIs and TINs as complementary tools in BO and PEP scrutiny. They help unambiguously identify legal entities and their transactions, and when combined with additional information, can assist in identifying the ultimate beneficial owner. This approach can enhance transparency and efficiency in financial transactions and trade activities while contributing to the overall integrity of the financial system.

An integrated innovative tools solution

In the section above, a number of critical building blocks, when used in conjunction with each other and existing tools and/or registers, can create an effective, holistic mechanism for BOT and PEP scrutiny, namely:

- Learning from the KYC utility and leveraging from existing registers by sharing information and therefore reducing the cost of compliance.
- Using social network analyses and identity matching as an effective tool to accurately identify institutions, individuals and their transactions.
- Capitalizing on powerful analytical tools including big data analytics, AI and ML.
- Leveraging digital identification, biometrics and SSI for individuals to create a backbone for any BO register, making it easier to identify individuals who are beneficial owners or PEPs.
- Taking advantage of the disruptive DLTs and blockchain that confer security benefits through their cryptography and their ability to facilitate transactions and store information in a transparent and tamper-proof way.
- Benefit from the existing identifiers for entities including the LEI, the TIN and the EORI numbers of registers.

The section above addressed the ‘what’ and ‘how’ these instruments can be used together as building blocks to develop an effective, innovative, holistic mechanism for BOT and PEP scrutiny in the future. This represents an ideal, TO-BE state, pro-actively addressing the FATF 40+ AML/CFT compliance requirements while enabling FIs, DNFBPs and various arms of government to scrutinise PEPs, and track and trace transactions belonging to the ultimate beneficial owner.

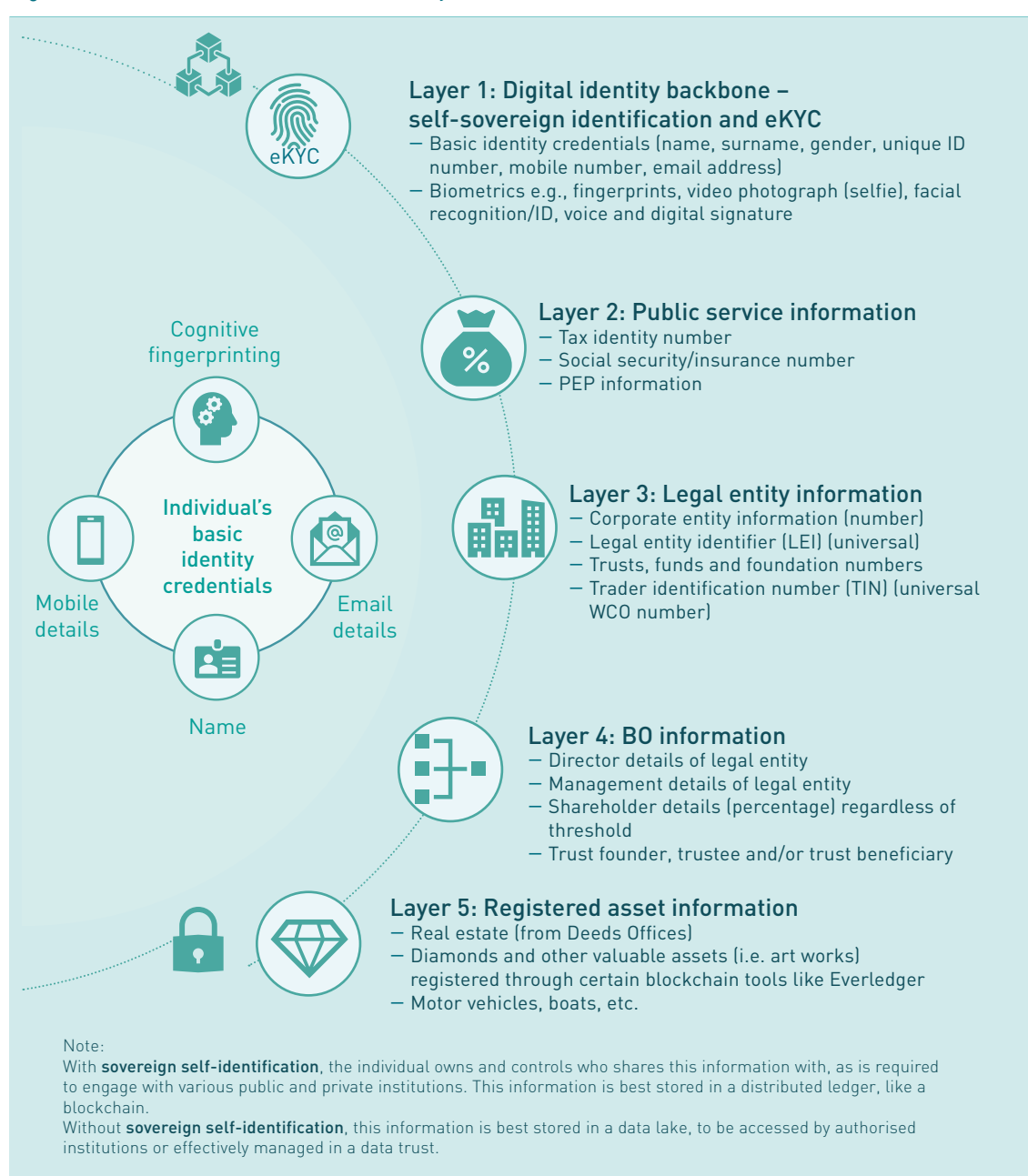
In this future, TO-BE environment, each added layer builds a composite profile of the individual (beneficial owner), similar to a payment stack, but rather this is a stack of different layers of identity credentials. The layers are summarized and include the following:

- **Layer 1:** the digital identity backbone, moving towards SSI and eKYC;
- **Layer 2:** public service information including PEP status;
- **Layer 3:** legal entity information, using a universal legal entity identifier, especially for entities that operate across borders and jurisdictions;

- **Layer 4:** BO information of all legal forms and the storage of share certificates; and
- **Layer 5:** registered asset information of all high-value assets and their ownership certificates.

As each layer is added to the holistic BOT and PEP scrutiny mechanism, a composite picture is created of the individual beneficial owner. While digital ID wallets using DLT or blockchain technology is proposed for the future BOT and PEP scrutiny mechanism, the *technology will more than likely evolve, and a better or alternate platform could be more suitable*. It is important to note that even implementing the immediate or short-to-medium term interventions (discussed below), it is possible to make significant progress regarding BOT and PEP scrutiny.

Figure 8: An innovative BOT and PEP scrutiny mechanism



The figure 8 illustrates how the various layers create a composite picture of the individual beneficial owner. In the immediate or short-to-medium term interventions, it means that the FIs and LEAs need to work together to *build* the composite profile by *stitching together the various layers of administrative data*. It is not necessary for all the data to be housed in one place – each overseeing government institution should house and maintain their own data, based on their own mandate. However, the real-time automatic exchange of information is necessary (usually through APIs) and critical to the success of any strategy aimed at curbing ML, TF, proliferation financing, IFFs and corruption.

This innovative, holistic BOT mechanism through progressive layering of information, ensures real-time, automatic exchange of interoperable information, through APIs, where FIs, Anti-Corruption Agencies, and LEAs collaborate to build comprehensive profiles of beneficial owners, integrating PEP registers and utilizing tools like big data analytics, AI&ML, and social network analyses for both proactive risk management and reactive law enforcement. These layers (as illustrated in Figure 8) are summarized below:

- **Layer 1 – Digital identity backbone and eKYC:** The foundation is a digital identity system, comprising basic identity credentials like name, gender, unique ID number, and biometrics such as fingerprints and facial recognition. Future developments may include embedding this information in a cryptographically secure DLT or blockchain, moving towards SSI and e-KYC. For countries without existing identity systems, collaborations with programmes like the World Bank’s ID4D can be a starting point. The goal is to shift towards digital identification with comprehensive biometric data, accelerated by advancements during the COVID-19 pandemic. ABSA bank’s involvement with the Sovrin Foundation exemplifies the shift towards SSI in the financial sector, simplifying identity management and promoting financial inclusion.
- **Layer 2 – Public service information including PEP status:** This layer adds public service information like tax identity numbers, social security numbers, and particularly PEP information from government payroll registers. In the future, as digital identification standards evolve, the need for specific numbers for various services may diminish, replaced by authentication through unique personal characteristics. Short-term measures include agreements for data sharing between government and law enforcement, with long-term goals focusing on interoperability and real-time verification.
- **Layer 3 – Legal entity information with universal identifiers:** This layer incorporates corporate entity information related to the individual, including ownership or directorship details, LEIs, and TINs. This facilitates trade and e-commerce across jurisdictions. Efforts should be directed towards standardizing identifiers like the global LEI and ensuring data interoperability for entities involved in international transactions. In the SSI future, individuals could store all related legal entity information in their digital ID wallets.
- **Layer 4 – BO information and share certificates:** This layer involves integrating information about directorships, management roles, shareholder details, and trust relationships into the individual’s profile. The use of DLTs could allow for the storage and

trading of share certificates. Immediate steps include creating BO registers, with longer-term goals of digitizing and automating this data for real-time access and verification.

- **Layer 5 – Registered asset information and ownership certificates:** The final layer involves storing high-value asset information, including real estate and valuable items, in digital ID wallets. This facilitates secure transactions and asset transfers. Building asset registers and standardizing database information are short-to-medium-term goals, while long-term objectives include enhancing security features for asset storage in digital wallets.

It is best to start with layer 1 and progressively build the subsequent layers on top of that, increasing the complexity of information available. The sequencing of these layers and their progressive implementation over time, detailed below, incrementally improve BOT and PEP scrutiny.

Layer 1: Digital identity backbone

The starting point is for an identity backbone, ideally, a digital identity backbone. Information to be included in the identity backbone are:

- Basic identity credentials (name, surname, gender, unique ID number, mobile number, email address); and
- Biometrics including fingerprints, video/photograph (selfie), facial recognition/ID, voice and digital signature.

In the not-so-distant future, this information can be embedded within a cryptographically secure DLT or blockchain, and may even capitalise on SSI wallets, using a single source of identity verification and authentication (such as a unique nationally issued identity document or passport). This addresses the protection of private information challenges. Where this is not possible, it is necessary to ensure that there is an existing identity number system in the country. If not, then engagement with the World Bank and its Integrated Identity Management and ID4D programmes, are a useful starting point. With digital technologies and smart phones, this will become less of an issue in the future, as individuals will be able to be identified using cognitive fingerprinting, on their mobile/digital devices.

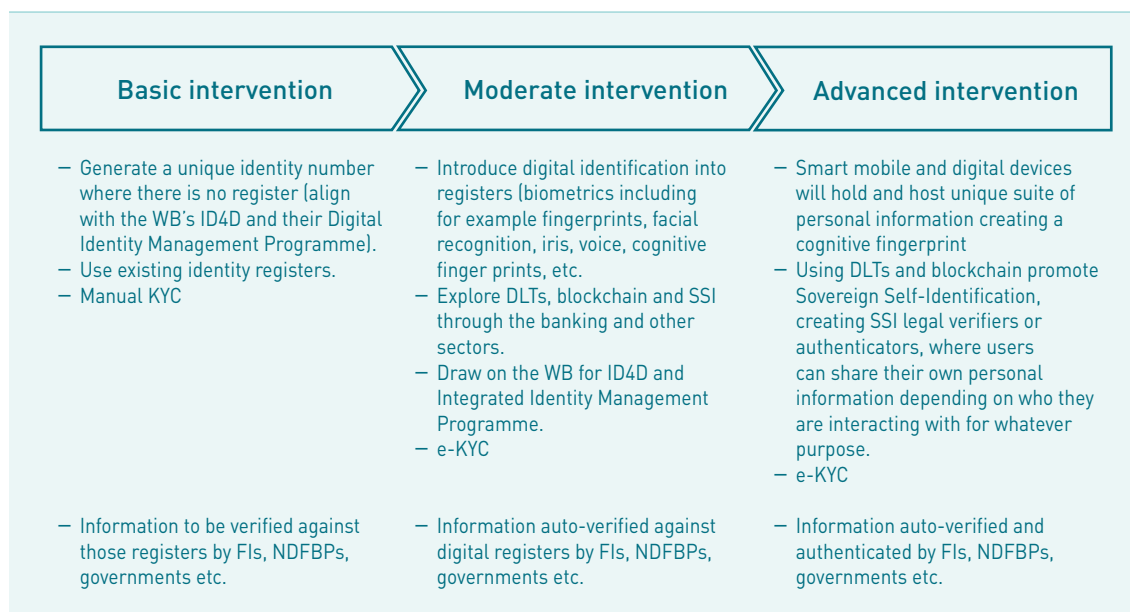
In the interim, for countries that do have existing identification registers, information can be verified against those databases (requiring data interfaces between institutions). The next step is to move towards digital identification attached to those registers, containing biometric information including a combination of fingerprints, facial recognition, iris, venous, voice, etc. The technology is moving at a rapid pace, thanks to the COVID-19 pandemic.

The ideal state is to progressively move towards SSI, using DLTs or blockchain. With e-commerce, the financial sector is progressively moving in this direction. ABSA bank in South Africa is the first bank in Africa to become a founding steward for the Sovrin Foundation, a global non-profit organization that promotes self-sovereign digital identification. There are numerous other players and digital identity should form the backbone of this BO stack, drawing on lessons from India's Aadhar system. Using DLT will help simplify identity challenges, enable clients to store

and update their personal information in a digital ID ‘wallet’, promoting e-KYC, lowering the transaction costs for protecting personal information, limiting cybercrime threats of identity theft and encouraging financial inclusion on the continent.⁶⁰

Using digital identification assists in addressing BOT and the scrutiny of PEPs as a useful AML/CFT tool. However, this tool cannot be used on its own: while it forms **the backbone of the solution**, it must be complemented by layering it with other data sources (e.g., corporate registries, LEIs, asset registers, PEP registers, etc.) and use tools such as social network analyses, identity matching, AI and ML, to analyse transactions for AML/CFT and anti-corruption purposes.

Figure 9: Digital identity backbone – interventions over time



Layer 2: Public service information

The next layer to add into the toolkit, is public service information, including, the individual’s:

- Tax identity number;
- Social security/insurance number; and
- PEP information, if they are public servants, documenting their position of office obtained from the government payroll register.

Additional layers of information could include unemployment insurance numbers or access to public sector grants, driver’s licence numbers etc. Using digital identity wallets, housing different government service numbers that unlock access to public services or confer rights, is beneficial to an individual, knowing that all their critical information is stored ‘safely’ in one place. As digital identification standards improve and becomes more widely used, the need for special numbers to access various services, will disappear, as authentication and verification of the individual will suffice to access these services. It is not inconceivable that in the near future, there will be no need

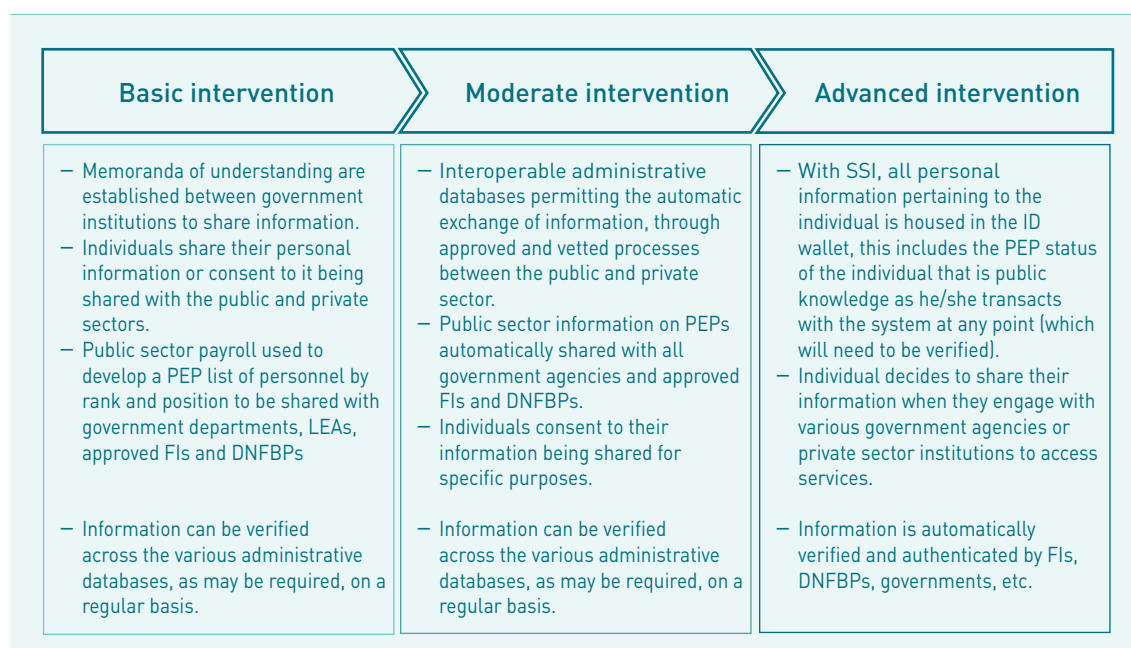
⁶⁰ Op. cit., Brun, et al., (2023).

for a separate tax number or social security number, it will all be driven by the salient suite of characteristics that ‘define’ individuals through cognitive fingerprinting.

As a minimum, this information can be made available between government authorities and approved private sector institutions. A list of PEPs should be drawn up from the government payroll, highlighting rank and position of influence. This should be made available to all government authorities, to utilize when approving public tenders, as well as approved financial institutions and DNFBPs. As a basic, short-term intervention, memoranda of understanding/agreement need to be signed between government institutions and law enforcement agencies to share and access this information.

As a short-to-medium term intervention, it is imperative that appropriate data standards are developed to ensure that the various administrative datasets and PEP register are interoperable and automatically exchanged electronically. Individual information needs to be checked and verified real-time. Over time, in the move towards digital identity wallets (either issued centrally by government or as decentralized solutions) using DLTs in the long run, the individual will share their personal information, as and when they need to transact with various entities across the system. Their PEP information should automatically be made available whenever they transact and should represent a condition of their service.

Figure 10: Public service information – interventions over time



Layer 3: Legal entity information

Much like the public sector information layer, this layer adds all the corporate entity information pertaining to the individual, making easier to assess the ultimate beneficial owner. Information included in the personal ID wallet of the individual includes the ownership or directorship of a corporate entity, providing the following:

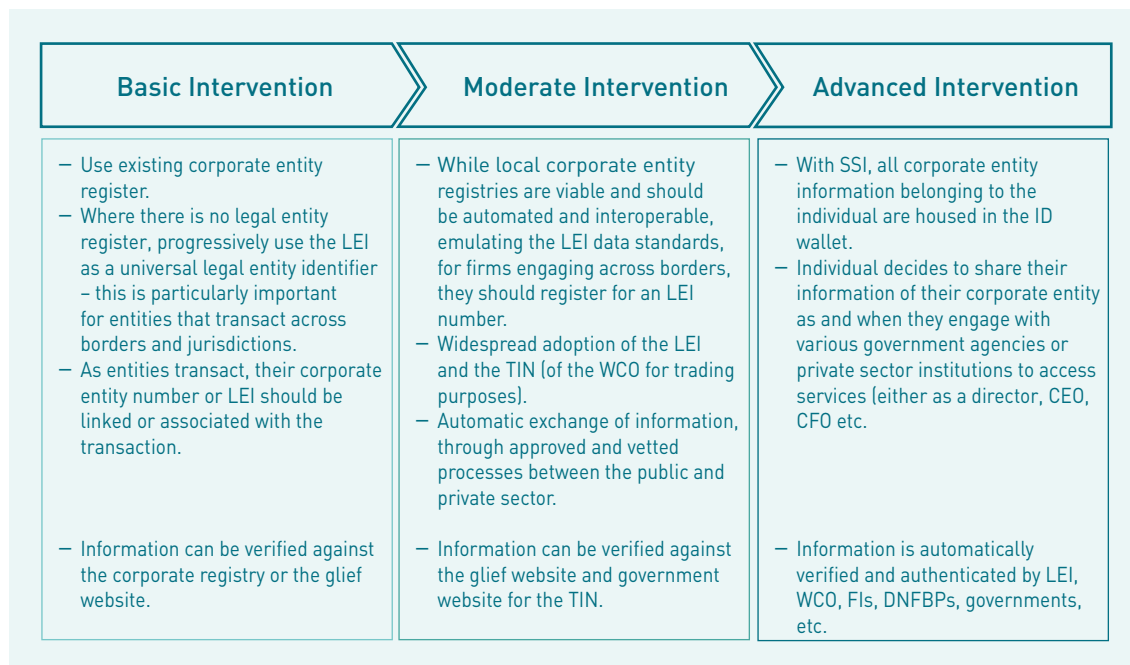
- Corporate entity information (number);
- Legal Entity Identifier (LEI)(universal); and even the
- Trader Identification Number (TIN)(universal WCO number).

This information facilitates trade and e-commerce, while enabling the entity to transact across jurisdictions and regions.

Over time, it is important to move towards one standard and the use of the LEI, might be the best legal entity identifier for entities that transact across borders. It is important that domestic governments who chose to retain their own corporate register for domestic firms, also store the LEI for the domestic firms with international transactions and activities. This ensures data interoperability and reduces the ambiguity pertaining to the identification and matching of legal entities that transaction across borders. For trade purposes, in the interim, the TIN is a useful trade identifier, but it is not clear which of the numbers will become more universally adopted. In time, there will only really need to be one entity, and with digitization, this will progressively be streamlined.

In the move towards digital identity wallets, the individual will want to house their personal information of the various legal entities owned or controlled within the digital ID wallet. This information will facilitate e-commerce and trade and will be beneficial to be easily accessible and shareable.

Figure 11: Legal entity information – interventions over time



Layer 4: BO information

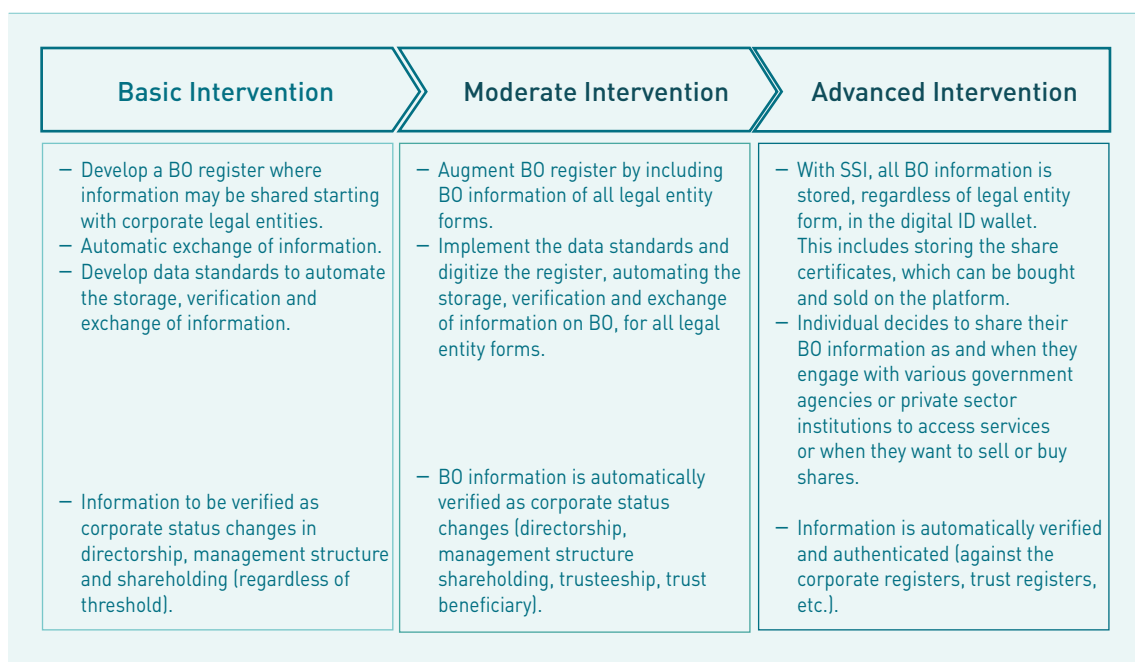
In the fourth layer, BO information is layered into the mechanism, containing the following information:

- Director details of legal entity;
- Management details of legal entity;
- Shareholder details (percentage) regardless of threshold; and
- Trust founder, trustee and/or trust beneficiary.

Here, the individual holds their personal information pertaining to their directorship, management role and shareholder details. This information should apply to all legal forms including, corporate legal entities, foundations, trusts, partnerships, etc. The advantage of DLTs and blockchain wallets is that it is even possible to store the share certificates in the wallet. Moreover, should the individual wish to sell their shares, they can do so and transfer the share certificates to the buyer. Thus, the key advantage of the longer-term solution is that individuals may store, and buy and sell their shares within the platform, adding to the benefit of digital ID wallets.

Immediate steps include the development of a central BO register. It is necessary to set up the various requirements such as memoranda of understanding/agreement (MOU/MOA) to share this information with other countries, FIs, DNFBPs, etc. Moreover, preparing the data standards for information to be exchanged is necessary. The short-to-long-term interventions include augmenting the register to include all legal entity forms and digitise the data so that it can be exchanged automatically, real-time to authorized and accredited users. This requires system and data standards to promote interoperability. In the long-term, the migration towards SSI or digital ID wallets, it is possible to even house share certificates and trade them as well. At this stage, information is updated as information changes, and this information is verified by trusted SSI vendors, the information is corroborated against the various legal entity registers.

Figure 12: BO information – interventions over time



Examples:

In **Austria**, a BO register was enacted under the 4th AML Directive pursuant to the Beneficial Ownership Register Law which came into force on 15 January 2018. The Austrian “WiERe” lists all Austrian corporate entities including private foundations. The founder (Stifter), the directors, and the beneficiaries have to be listed. In addition, specific category of beneficiaries are also included as so-called “one-time beneficiaries” (Einmalbegünstigte) who receive a distribution in excess of EUR 2,000 in a certain calendar year, should be listed for the calendar year in which they have received a distribution.

Austria has enacted the 5th AML Directive on 10 January 2020, the BO information of companies and private foundations is now available to the general public with no restriction. Austria’s beneficial owner register has a high level of automation which includes:

- automated real time cross-checks against government databases;
- automated sanctions in case information are missing;
- a public remark to warn users that a company has potentially incomplete or wrong information; and
- a system of risk points for non-resident beneficial owners based on their country of residence’s risk automated coercive penalties.

In **Denmark**, the Danish beneficial owner register is integrated into the Central Corporate Registry and National Register of citizens with a Danish social security number (CPR-number). When a Danish person is registered as a director, board member, beneficial owner, legal owner or founder, the system automatically retrieves information from the National Register, and run a series of checks. The system can detect and alert if the person is deceased; missing; has not registered an address; or is under the age of 18. The BO information can be accessed online in open data format.

In **Australia**, Austrac provides details on how information and guidance on how information should be collected by financial institutions and DNFPBs in meeting their FATF compliance requirements.

This includes:

- Documenting procedures;
- Determining who beneficial owners are;
- Assessing beneficial owner’s ML or TF risk;
- Information to be collected and verified;
- Record-keeping;
- Expectations, discrepancies and alternate individuals if the beneficial owner cannot be identified.

More on this can be found at <https://www.austrac.gov.au/business/how-comply-and-report-guidance-and-resources/customer-identification-and-verification/beneficial-owners>.

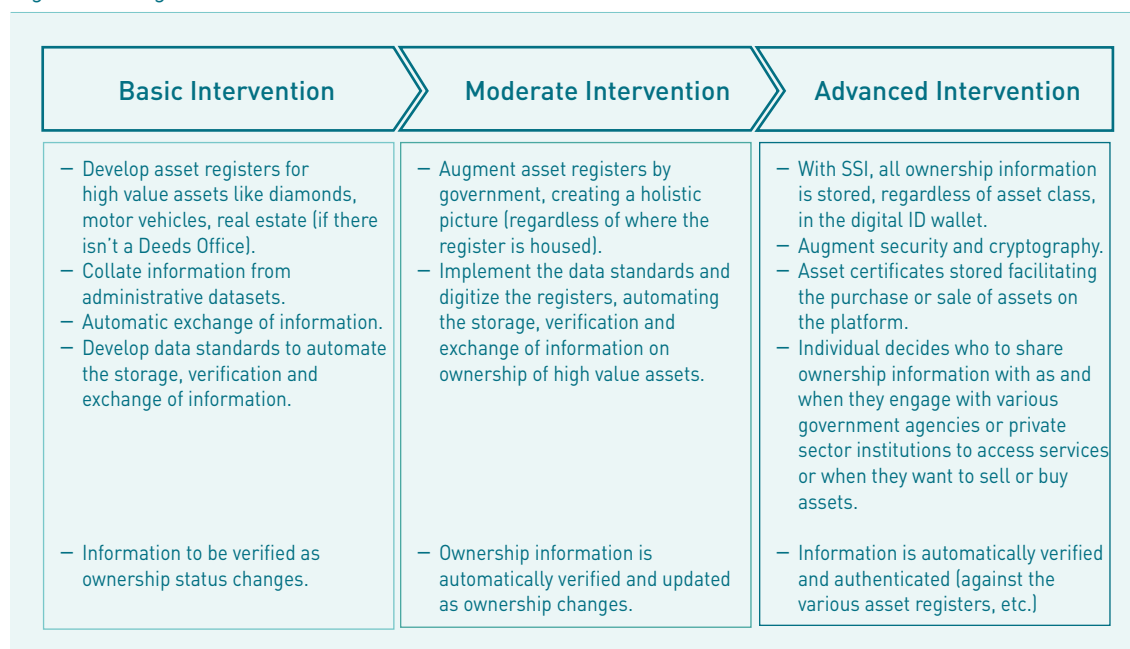
Layer 5: Registered asset information

The final layer in the BO holistic toolkit for the future, is that asset information can be stored and contained in the digital ID wallet, including:

- Real estate (from Deeds Offices)
- Diamonds and other valuable assets (i.e. art works) registered through certain blockchain tools like Everledger or Provenance
- Motor vehicles, boats, etc.

Since DLTs can facilitate transactions, it is possible to add the feature of buying and selling assets on the register or platform. Once again, this information can be shared with various institutions when the individual chooses to transact.

Figure 13: Registered asset information – interventions over time



Most countries do not have asset registers for high-value items, such as gold, diamonds, art etc. It is important to build various asset registers and standardize the information on the database to facilitate the automatic exchange of information. Over the short-to-medium term, it is necessary to augment the various registers, drawing on the various administrative datasets. For example, it is not necessary to compel citizens to register their motor vehicles in a separate register. The government can utilize the motor vehicle license registration process to compile an asset ownership list for use by various authorized and accredited government (i.e. LEAs), financial institutions or DNFBPs who require the information to prevent AML/CFT. As this information is automated, it is possible to share the information real-time with accredited users. It is not necessary for the asset registers to reside in one institution at this point – it should be housed in the various overseeing government authorities, for example, the department of minerals or mining would have the asset registers related to precious metals and stones, whereas the department of transport will have the motor vehicle register, etc.

In the long-term, through SSI or digital ID wallets, the individual can house all their asset certificates within their digital ID wallet, where the platform may also be used to buy and sell the assets. Security and fidelity at this stage are critical to ensure that each wallet remains secure. One idea might be that each digital ID has sub-categories for the various classes of personal information stored, with added security for the share certificates and registered asset classes. This could include cold wallets or wallet safes in the future.

In summary, the *innovative transparency mechanism* outlined above represents a possible approach to promoting transparency creating an integrated 'registry' with a composite profile of the beneficial owner. As digital identity becomes more decentralized, the innovative transparency

mechanism allows the individual to own and hold their identify information and share it on a need-to-know basis as it is related to the ability to transact.

Unexplained wealth orders (UWOs)

The Unexplained Wealth Orders (UWOs) system is a legal framework that allows authorities to investigate and potentially confiscate assets that are disproportionate to a person's known sources of income. UWOs are a type of investigative and confiscation procedure that require certain persons to show how they obtained certain property once authorities have shown it to be disproportionate to their lawfully obtained income and assets. UWOs may apply to any person, including legal persons, or specifically target PEPs. The rationale for implementing UWOs revolves around their potential to uncover and address unexplained wealth, combat financial crime, enhance transparency, and contribute to the recovery of illicitly obtained assets. By requiring individuals to account for their wealth through legitimate means, UWOs play a crucial role in promoting financial integrity and accountability.⁶¹

The UWO system requires the enactment of legislation that formally introduces the concept of UWOs into the legal system. This legislation outlines the criteria for the issuance of UWOs, the procedural requirements for their application, and the legal consequences of non-compliance. Furthermore, oversight, protection of the rights of respondents, limitations on the use of disclosed information, and mechanisms for independent oversight of the UWO framework are also necessary inclusions. Establishing procedural safeguards is crucial to ensure that the use of UWOs is balanced and respects the rights of the individuals subject to these orders. This may involve provisions for judicial oversight, protection of the rights of respondents, limitations on the use of disclosed information, and mechanisms for independent oversight of the UWO framework. The legislation should outline the enforcement mechanisms available to authorities once a UWO is issued. This may include provisions for compelling the production of information on the origin of certain assets, as well as the legal consequences for non-compliance, such as potential confiscation of assets.

Tax crime investigation maturity model

One innovative tool in the fight against financial crimes is the Tax Crime Investigation Maturity Model developed by the OECD.⁶² This self-assessment diagnostic tool helps jurisdictions understand their level of implementation of the OECD's *Fighting Tax Crime – The Ten Global Principles*. By providing indicators for increasing levels of maturity, the model charts an evolutionary path for progress towards cutting-edge practices in tax crime investigation. It assesses inter-agency coordination domestically and internationally, covering the entire law enforcement process from initial intelligence gathering to the recovery of criminal proceeds. Additionally, the model specifically examines the effectiveness of inter-agency coordination for countering

⁶¹ Op. cit., Brun, et al., (2023).

⁶² Ibid.

IFFs, contributing to more effective intelligence gathering and analysis, and improvements in cooperation and information sharing between government agencies and across countries to prevent, detect, and prosecute financial criminals.

Inter-agency centres of intelligence and fusion centres

Inter-agency centres in the form of fusion centres and centres of intelligence entail the inclusion of one representative or more from each unit engaged in investigative efforts and information sharing. This integrated approach combines inter-agency resources and enables sharing of information within the boundaries of the law. For example, the National Criminal Intelligence Fusion Centre in Australia was launched in 2010 to bring together information, skills, knowledge, data, and technology across government departments.⁶³

Inter-agency Centres of Intelligence and Fusion Centres are critical components of a comprehensive approach to combating ML and other financial crimes. These centres bring together representatives from various government agencies, including law enforcement, intelligence, and regulatory bodies, to share information and coordinate efforts to identify and disrupt illicit financial activities.

Inter-agency Centres of Intelligence are designed to facilitate the sharing of intelligence information between different government agencies. These centres serve as a hub for the collection, analysis, and dissemination of intelligence information related to financial crimes. By bringing together representatives from different agencies, these centres can help identify patterns and trends in illicit financial activities, as well as provide a more comprehensive understanding of the scope and scale of these activities.

Fusion Centres, on the other hand, are designed to facilitate the sharing of information between different government agencies at the operational level. These centres bring together representatives from different agencies to share information and coordinate efforts to identify and disrupt illicit financial activities. Fusion Centres can help identify emerging threats and trends, as well as provide a more comprehensive understanding of the scope and scale of illicit financial activities.

Both Inter-agency Centres of Intelligence and Fusion Centres are critical components of a comprehensive approach to combating ML and other financial crimes. By facilitating the sharing of information and coordinating efforts between different government agencies, these centres can help identify and disrupt illicit financial activities, ultimately contributing to a safer and more secure financial system.

⁶³ Ibid.

Public-private partnerships

Public-private partnerships (PPP) can play a crucial role in the development and implementation of technology-based solutions. These partnerships can facilitate the sharing of data and expertise between the public and private sectors, as well as the development of innovative solutions to combat IFFs.

PPP can play a crucial role in the implementation of UWOs systems by facilitating information-sharing and cooperation between public and private entities. FIs, for example, can provide valuable information and expertise to LEAs in identifying suspicious transactions and potential cases of unexplained wealth. In turn, LEAs can provide guidance and support to financial institutions in complying with UWO regulations and reporting requirements.⁶⁴

Cybersecurity and data protection

The use of technology solutions also poses cybersecurity risks that must be addressed. It is essential to develop robust cybersecurity measures to protect against cyber threats and ensure the integrity and confidentiality of data (UNODC, 2021). Robust security controls and monitoring mechanisms need to be implemented to detect and prevent cyber threats, such as malware, phishing, and ransomware attacks. This includes deploying firewalls, intrusion detection and prevention systems, and security information and event management (SIEM) tools to monitor network activity and detect anomalies.⁶⁵

In addition, ensuring compliance with data protection and privacy regulations, such as the General the data protection regulations, is essential. This includes implementing appropriate technical and organizational measures to protect personal data, such as encryption, access controls, and data minimization.

Managing the risks associated with third-party service providers, such as cloud providers or data processors, is essential for safeguarding sensitive data. Given the sensitivity of the information involved, it's crucial to implement robust measures to ensure the security and confidentiality of data when it is accessed or processed by third parties.

Developing and implementing incident response and business continuity plans is crucial for ensuring the resilience of data systems in the face of cyber attacks or other disruptions. These plans are designed to enable the systems to effectively respond to and recover from security incidents, minimizing the impact on operations and data integrity.⁶⁶

64 Ibid.

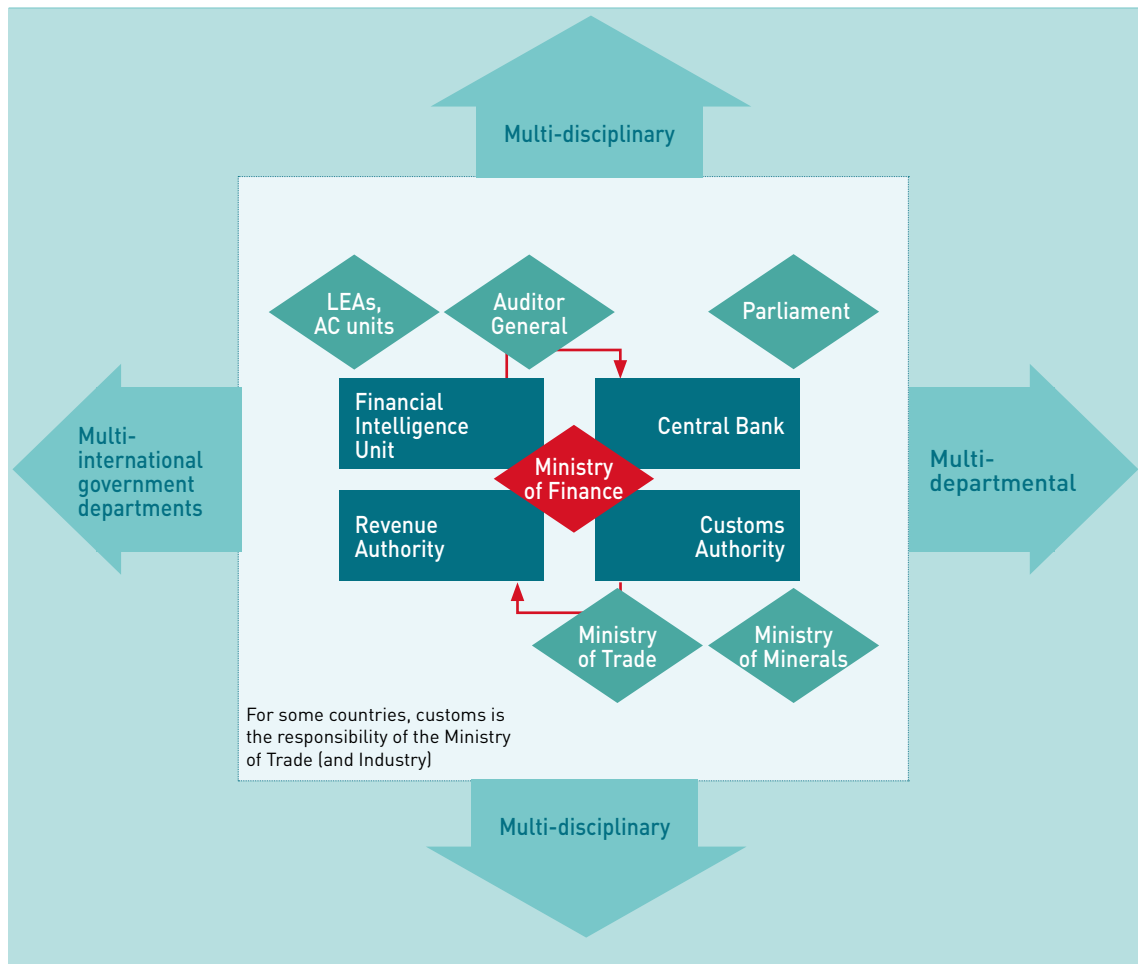
65 Ibid.

66 Ibid

Processes: technical framework

The next step in the entire toolkit relates to the processes and procedures that need to be implemented, relating specifically to the technical framework. Effectively addressing IFFs, ML and TF as well as corruption, necessitates a multi-disciplinary, multi-stakeholder, and multi-jurisdictional approach that encompasses the efforts of the public, private, and civil society sectors. This holistic approach is essential for combating the complex and cross-cutting nature of illicit financial activities, requiring collaboration and coordination across various domains and entities to achieve meaningful impact. The figure below illustrates the complexity of addressing BOT and PEP scrutiny, as it requires: collaboration across a multitude of departments, LEAs and anti-corruption (AC) units within a country's borders as well as with entities in other countries or jurisdictions. Navigating this complex space also requires officials from LEAs, AC agencies and supreme audit institutions to be well-versed across a number of disciplines, from the economics of crime, to tax and accounting, trade and law and trade.

Figure 14: A multi-disciplinary, multi-stakeholder and multi-jurisdictional approach for addressing IFFs



In addition to the technical framework, it is imperative to emphasize the role of advanced technologies such as big data analytics, AI and ML in enhancing the capabilities to detect, prevent, and mitigate IFFs.⁶⁷ These technologies can provide sophisticated tools for analysing vast

⁶⁷ <https://gfmag.com/features/de-risking-technology-aml/#:~:text=Fixing%20AML%3A%20Can%20New%20Technology,solve%20the%20de%2Drisking%20problem.>

and diverse datasets, identifying patterns of suspicious financial activities, and strengthening the overall resilience of the AML/CFT financing efforts. By integrating these advanced technological solutions within the multi-disciplinary approach, a more robust and adaptive framework can be established to address the evolving challenges posed by IFFs.

Guidelines, processes and procedures

Guidelines are an essential tool for organizations, both public and private, to standardize practices and streamline processes into a set of sound and routine steps. They aim to use evidence-based lessons learned and best practices to create a statement that determines a course of action. Guidelines can be issued and used by any organization to make the actions of its officials or divisions more predictable and of higher quality. They are like rules, but guidelines are more flexible and adaptable to different contexts.

To effectively combat IFFs, different guidelines or processes (and procedure manuals) should be developed for officials in various government institutions, regulatory and supervisory bodies, financial institutions, DNFBPs, and the public at large. Detailed procedure manuals should be developed for officials who work closely in the BO and PEP transparency framework. These procedures should also address unilateral and multilateral stakeholder engagement.

The Inter-Departmental Task Force should include representatives from a wide range of government institutions and non-profit organizations that have a direct role to play in AML/CFT, curbing IFFs and commercial tax malpractices, and anti-corruption. The Task Force has several policy levers available to address these issues.

The figure shows the components of a framework aimed at countering IFFs and enhancing transparency. These components include:

- **AC, IFFs and AML/CFT:** connected to an “Inter-Departmental Task Force,” indicating a coordinated approach to combating corruption, ML, and the financing of terrorism.
- **Open government contracting and public procurement (EITI, LEI):** the use of initiatives like the Extractive Industries Transparency Initiative (EITI) and Legal Entity Identifier (LEI) to promote transparency in public contracts and procurement.
- **UWOs:** targets wealth that cannot be explained by known legal income sources, likely as a measure to combat corruption and ML.
- **Illicit enrichment asset declarations (PEPs):** the need for PEPs to declare assets as a preventive measure against illicit enrichment.
- **Lifestyle audits (public officials):** regular audits of the lifestyle of public officials to detect any discrepancies with their legal income.
- **BO and PEP transparency (natural persons, legal persons and legal arrangements):** the transparency of BO and the relationships of PEPs, applicable to individuals, companies, and legal arrangements.
- **Asset confiscation, recovery and forfeiture (conviction and non-conviction-based):** mechanisms for seizing and recovering assets derived from or used in criminal activity, regardless of a conviction.

- **Exchange of information on request (EOIR) and country-by-country reporting:** EIOR and Country-by-Country reporting, are critical to address tax evasion and base erosion and profit shifting.
- **Tax and customs investigations:** the investigation procedures for tax and customs-related crimes.
- **Voluntary tax disclosure programmes (VTDPs):** programmes that allow individuals or entities to voluntarily disclose previously undeclared taxes.

Risk analysis and assessments to determine threats and implement solutions

Risk assessment is the first step in implementing a RBA that shifts risk management from the regulator to the one being regulated – the entity. The aim of a national risk assessment is to support entities, institutions, businesses and professionals to conduct their own risk assessments. Risks can be seen as a function of 3 factors: threat, vulnerabilities and consequences. A deficient risk assessment at any stage of the process will have a cascading effect.

Supervisory authorities should adopt a RBA to supervising financial institutions' AML/CFT systems and controls, based on the ML and TF risks present in a country. The frequency and intensity of on-site and off-site AML/CFT supervision of financial institutions/groups should be consider the policies, internal controls, and procedures associated with the institution/group, as identified by the supervisor's assessment of the institution/group's risk profile. The implementation of risk analysis and assessments involves identifying and assessing risks, adopting a risk-based approach, supervising financial institutions, and implementing risk management and mitigation measures. These steps are crucial to effectively combat ML and TF.⁶⁸

Risk-assessment tools, to mention a few, include: World Bank; International Monetary Fund (AML/CFT); CENFRI (Financial Inclusion and AML/CFT); GIZ – Country Risk Profile on IFFs for governments; GIZ – Inter-departmental Working Group's BOT Risk Assessment Tool; and SARB MVTS Interactive Risk Assessment Tool (money value and transfer services interactive tool).

Key components of the ML/TF Risk Assessment Toolkit include:⁶⁹

- Step-by-step guidance for conducting a risk assessment, including entity risk assessment and BOT assessment.
- Network diagrams for assessing national vulnerability, which cover factors such as the quality of corporate registries, effectiveness of enforcement of sanctions/fines, and international information exchange.
- Instructions for adapting the assessment indicators based on national context and specific risk factors not included in the template.
- Recommendations for sharing the results of the assessment widely across the public sector and with key private sector and civil society partners, with necessary redactions for sensitive information.

⁶⁸ Op. cit., FATF (2023b)

⁶⁹ World Bank. (2022). *Legal Persons and Arrangements ML Risk Assessment Tool: With guidance on assessing risks related to beneficial ownership transparency.*

Many countries have a national risk assessment that is undertaken annually (a FATF requirement for AML/CFT). These risk assessment tools provide a heat-map of where the key threats and risks exist across the landscape. The Inter-Departmental Task Force needs to use the information from the risk assessments and develop strategies to mitigate those risks. Identifying the risk and determining the strategy or solution followed by an action plan to remedy the threat or risk underpin the FATF's risk-based approach.

In the case of public officials' asset and interest declarations, implementation of automated risk analysis plays an important role in curbing IFFs.⁷⁰ By employing automated risk analysis, using predetermined risk indicators, the system can effectively raise "red flags" or indicators of potential risk, thereby signaling the need for further review by government agencies. This approach streamlines the verification process and enables the identification of high-risk declarations that warrant closer scrutiny, and also allows for the review of a large volume of declarations, which may not have been feasible through manual intervention alone. This underscores the pivotal role of automated risk analysis in enhancing the efficiency and effectiveness of the verification process.

The development of the risk analysis framework includes preparation stage, data extraction stage, data exploration stage, and rules testing stage as integral components of the framework development process. The preparation stage involves laying the groundwork for the risk analysis, while the data extraction stage focuses on obtaining the necessary data from the declarations. Subsequently, the data exploration stage entails the in-depth examination of the extracted data, and the rules testing stage involves validating the risk analysis rules. Additionally, the guide emphasizes the need for integration with external data sources, highlighting the importance of accessing structured information from external sources to enhance the effectiveness of the risk analysis. This integration enables a more comprehensive assessment by cross-referencing the declaration data with external datasets, thereby strengthening the risk analysis process.

Collect, verify and store information

Ensuring the accuracy and timeliness of BO information is essential for maintaining the integrity of disclosure regimes and increasing trust in the transparency of corporate entities. To achieve this, initial registrations and subsequent changes to BO must be promptly submitted, and the information should be updated within a clearly defined timeframe following any alterations. Several key considerations should guide the collection, storage, verification, and updating of BO and PEP information.

Firstly, data accuracy should be confirmed at least annually, and all changes in BO must be reported. Additionally, creating an auditable record of BO by dating declarations and storing historical records is crucial for maintaining transparency and accountability.

⁷⁰ Dmytro, K., and L. Pop. (2021). *Automated Risk Analysis of Asset and Interest Declarations of Public Officials A Technical Guide*. Available at <https://star.worldbank.org/publications/automated-risk-analysis-asset-and-interest-declarations-public-officials>.

Requiring the timely submission of changes to ownership data or details of natural or legal persons enhances confidence in the currentness of the data and reduces the risk of misrepresentation by legal entities. Regular updates should encompass all changes that have occurred since the last declaration, thereby preventing companies from disguising short-term changes in BO and closing potential loopholes for non-disclosure.

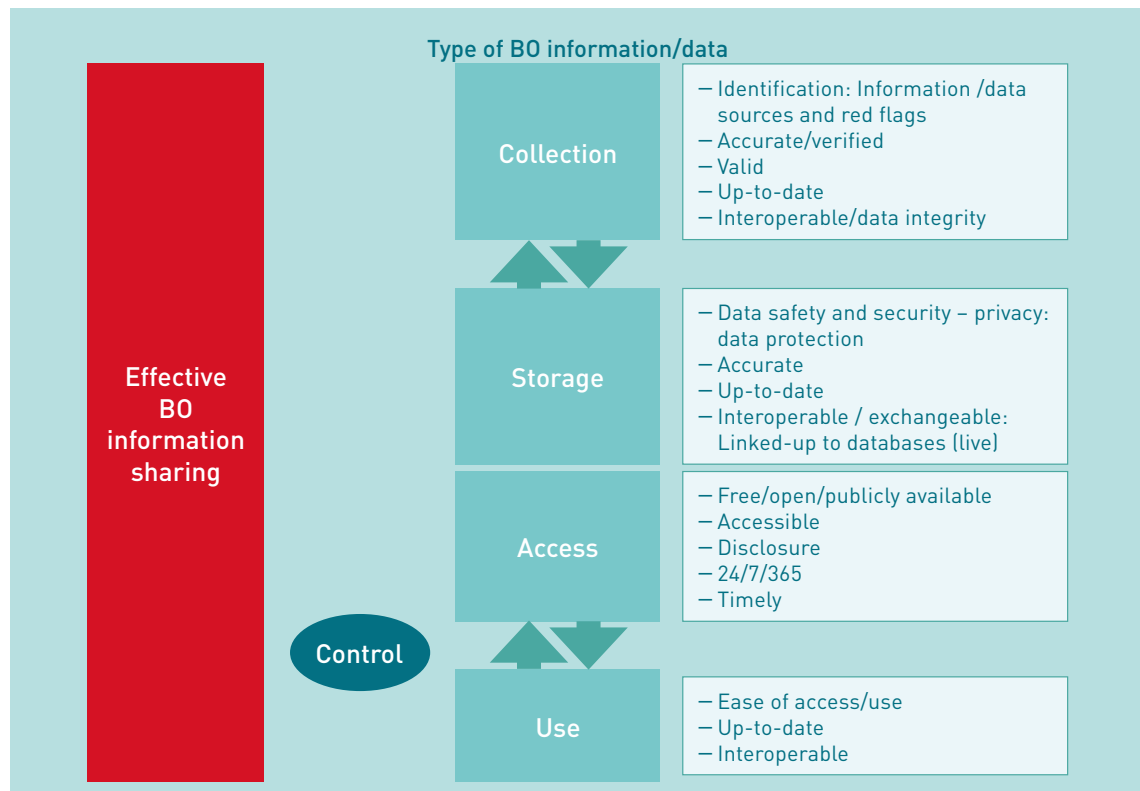
Furthermore, the development of a RBA for assessing, determining, collecting, and verifying information on beneficial owners is essential. This approach ensures that the level of scrutiny applied to BO information is commensurate with the associated risks, thereby optimizing the allocation of resources for due diligence.

Retaining historical information about companies is equally important, as it can reveal connections that may not be immediately apparent from current information. This practice prevents entities from obscuring their identities through name changes and facilitates investigations in complex legal cases.

Moreover, making supporting information, such as the date of a BO declaration, available to users can aid in assessing the reliability of the information and provide evidence of the timing of due diligence activities, particularly in cases requiring retrospective scrutiny.

The figure below illustrates the data requirements associated with the collection, storage, access and use, so that the BO information (in a public central registry), is interoperable, available real-time, accessible and more importantly shareable across entities within a country and across borders, in other jurisdictions.

Figure 15: Effective BO information sharing



Monitor, analyse and enforce: monitoring, evaluation and learning framework

The cornerstone of the Monitoring, Evaluation, and Learning Framework (MERL) lies in the critical functions of monitoring, analysis, and enforcement. Simply accumulating information without maintaining, analysing, and utilizing it serves no meaningful purpose. It is imperative to extract valuable lessons from the entire monitoring, analysis, and enforcement processes and consistently implement relevant changes. This involves regularly refining and adapting the mechanism to keep pace with a dynamic and evolving world, while also staying abreast of the latest analytical tools. This ensures that the framework remains current, agile, and responsive to emerging challenges and opportunities.

Moreover, the iterative nature of the monitoring, evaluation, and learning process should be emphasized, as it is the mandate of all competent authorities and LEAs, anti-corruption agencies and special investigating units. Establishing continuous feedback loops facilitates ongoing improvements and adjustments based on real-time insights and changing circumstances. This iterative approach enables the framework to evolve in tandem with the evolving landscape of financial crimes and ML, thereby enhancing its effectiveness and relevance over time.

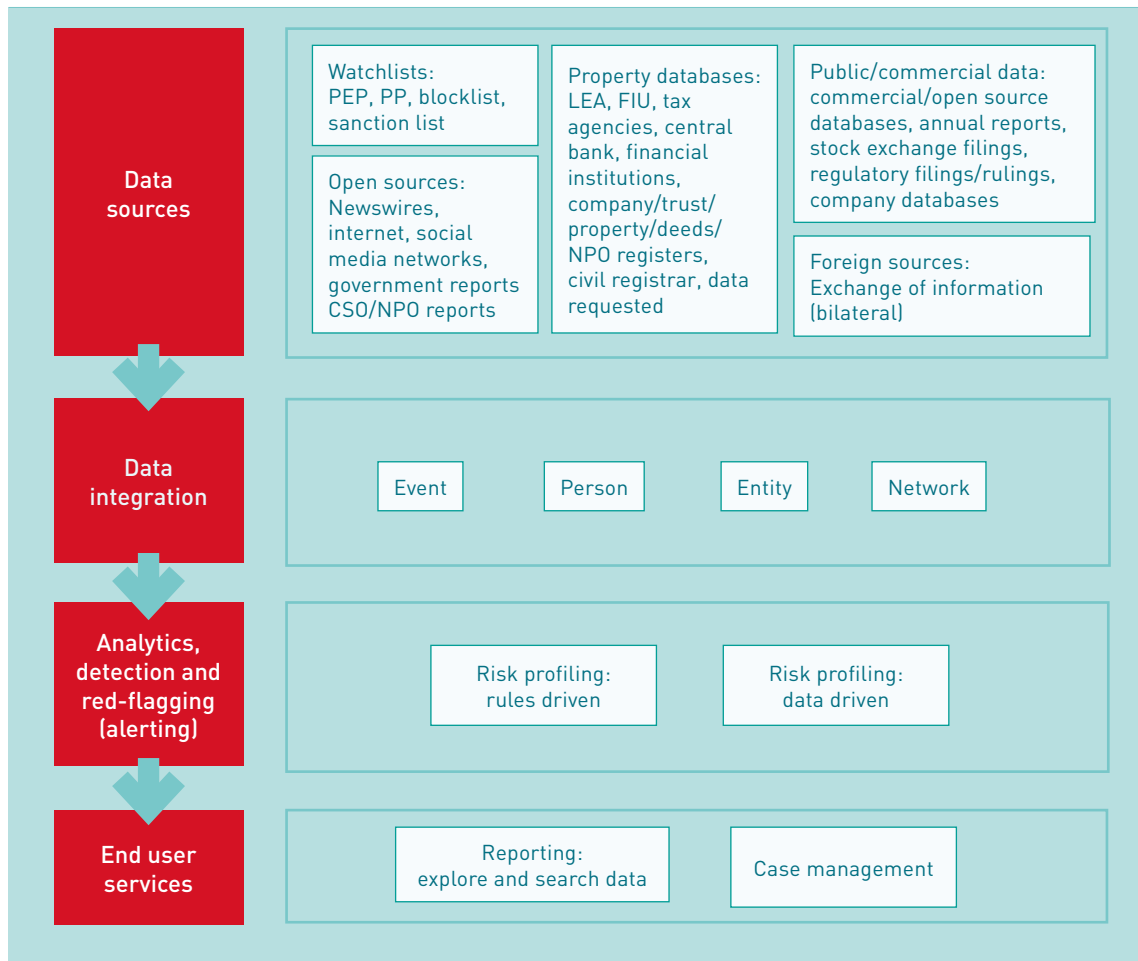
Furthermore, advanced technologies and data analytics plays a pivotal role in bolstering the monitoring and analysis capabilities within the framework. Leveraging cutting-edge analytical tools and technologies enables the identification of complex patterns and trends, thereby enhancing the framework's capacity to detect and respond to emerging threats and illicit activities.

Tracking, tracing and analysing BO and PEPs

After the data has been collected, the next crucial step is to monitor the information by tracking, tracing, and analysing it. This involves verifying the information and utilizing various tools such as big data analytics, AI and ML, social network analyses, and chain analyses to understand the relationships between natural persons, entities, networks, and events such as transactions. Analyses that carefully stitch together BO relational networks across entities and jurisdictions, highlighting PEPs where relevant, are a powerful and useful tool for investigative purposes. These tools should be developed by the various competent authorities: a decision needs to be made whether the intelligence elements are going to reside in multiple agencies or a single agency such as the FIU. Leveraging skills and expertise from the private sector and Non-Profit Organizations of CSOs would be important.

This is an ongoing process that needs to be conducted regularly as changes in ownership occur, ensuring that the network relationships (chain links or analyses) are accurate and current in real-time. Analysing this information is critical, as it enables the red flagging of possible threats and risks, as well as from a case management (investigation) perspective.

Figure 16: A value chain to optimize the use of information for BO and PEP transparency



The tracking, tracing, and analysis value chain is illustrated in Figure 16, highlighting the importance of utilizing advanced technologies and data analytics in monitoring and analysing financial transactions and ownership structures. By leveraging these tools, it becomes possible to identify and respond to emerging threats and illicit activities, ultimately enhancing the effectiveness of the framework in combating financial crimes.

In addition to the above, maintaining the confidentiality and security of the collected data is a must. This involves implementing robust data protection measures, including encryption, access controls, and secure storage, to safeguard sensitive information from unauthorized access or disclosure. By ensuring the confidentiality and security of the collected data, the framework can maintain the trust and confidence of stakeholders, including FIs, LEAs, and the public at large.

Investigate

The data analysis process of tracking, tracing, and analysing the data generates exceptions that require red flagging. These red flags necessitate human intervention (investigation) to assess whether the case is suspicious enough to warrant further analysis and digging deeper. If a formal investigation is triggered, the financial intelligence centre or other relevant institution (such as the Anti-Corruption Unit) must work with LEAs to further investigate the case. Case management

is typically a process managed by LEAs in conjunction with the financial intelligence centre, tax authority, and central bank.

The investigation process is a critical component of the MERL Framework. Investigating suspicious cases requires a high level of expertise and resources, including specialized skills, tools, and technologies. Therefore, it is essential to ensure that the relevant institutions have the necessary resources and capabilities to conduct effective investigations.

The Task Force should have oversight over the suspicious cases/investigations handed over to LEAs, reporting to the highest levels of government. This acts as an independent audit of the information handed over, creating lines of accountability, particularly when it relates to corruption. The Task Force's oversight role ensures that the investigations are conducted in a transparent and accountable manner, thereby enhancing public trust and confidence in the framework.

Consider the following for internal government use:

- What type of investigation and case management is going to be undertaken?
- Which institution will be responsible for investigations: red flags from the database; and suspicious cases?
- What type of analysis, case management and investigation are to be undertaken by the institution responsible for managing the register?
- What collaboration/cooperative governance structure needs to be put in place to share data, investigate and prosecute cases?
- What type of capacity is required for the investigation?
- What is the role of the Task Force in managing investigations?
- What reports will be sent to the highest levels of government on cases handed over the LEAs?

Enforce and prosecute

It is crucial to utilize the monitoring, tracking, and tracing information to gain insights into non-compliance from a disclosure perspective. Effective, proportionate, and dissuasive sanctions or penalty regimes must be in place for non-compliant disclosures, encompassing late, incomplete, false or non- submission.

Diverse sanctions should be applied to address the different parties disclosing the information or making the declaration, such as the beneficial owner, registered officers of the company, and the company making the declaration and/or the PEP. These sanctions should encompass both monetary and non-monetary penalties, potentially impacting certain business-related rights, such as the inability to incorporate a company or receive dividends from shares. It is essential for relevant agencies to be empowered and resourced to enforce the sanctions imposed for non-compliance.

For sanctions to act as an effective deterrent, they must be fairly and proportionately enforced in practice. To achieve this, relevant agencies need both the legal mandate and adequate resources

to identify suspected non-compliance, conduct appropriate investigations, and issue sanctions. The presence of adequate sanctions and their effective enforcement serves to enhance disclosure compliance and improve the quality and utility of the data. Including sanctions against the beneficial owner, registered officers of the company, and the company making the declaration helps ensure that the deterrent effect of sanctions applies to all key persons and entities involved, incentivizing compliance from all stakeholders engaged in the governance and management of the company. Enforcement without prosecution or relevant sanctions renders the entire mechanism a waste of time and resources.

Social audits

Social auditing is a vital process for evaluating, reporting on, and enhancing an organization's performance and behaviour, as well as measuring its impact on society. This comprehensive approach involves all stakeholders and entails systematically and regularly monitoring performance while considering the perspectives of stakeholders. Transparency in reporting any issues affecting the public is a fundamental aspect of social auditing. As noted, "Social audits allow people to enforce accountability and transparency, providing the ultimate users of services and projects with an opportunity to scrutinize development initiatives. It is a form of citizen advocacy based on the power of knowledge and is grounded in the right to information".⁷¹

In the context of combating ML and the financing of terrorism, social auditing can play a crucial role in promoting transparency and accountability within financial institutions and DNFBPs. By engaging all stakeholders and systematically monitoring their performance, social auditing can help identify and address potential vulnerabilities to ML and TF. Furthermore, by providing a platform for the public to scrutinize and advocate for the integrity of financial systems, social auditing can contribute to the overall effectiveness of AML/CFT efforts.

Service, staff, skills and resources: resource framework

The effective implementation and operationalization of a national strategy and action plan for BO and PEP transparency require a robust resource framework. This framework encompasses the service, staff, skills, and resources necessary to establish a comprehensive mechanism that goes beyond the mere disclosure framework.

The service component of the resource framework refers to the provision of adequate support services to facilitate the implementation of the national strategy and action plan. This includes the provision of technical assistance, training, and capacity building to relevant stakeholders, such as FIs, DNFBPs, and regulatory authorities. Additionally, the provision of support services

⁷¹ Eavani, F., Nazari, K., & Emami, M. (2012). Social audit: From theory to practice. *Journal of Applied Sciences Research*, 8, pp. 1174–1179.

to the public, such as helplines and online resources, can enhance the effectiveness of the mechanism.

The *staff* component of the resource framework refers to the availability of skilled personnel to implement and operate the mechanism. This includes the recruitment and training of personnel with the necessary expertise in areas such as data analysis, risk assessment, and investigation. Furthermore, the availability of personnel with language skills and cultural competencies can enhance the effectiveness of the mechanism in diverse contexts.

The *skills* component of the resource framework refers to the development and enhancement of the necessary technical skills to implement and operate the mechanism. This includes the development of skills in areas such as data management, risk assessment, and investigation. Additionally, the development of skills in emerging areas such as AI and ML can enhance the effectiveness of the mechanism.

The *resources* component of the resource framework refers to the availability of financial and technological resources to implement and operate the mechanism. This includes the provision of adequate funding to support the implementation and operation of the mechanism, as well as the availability of technological resources such as software and hardware to support data management and analysis. Budgeting for the BO and PEP transparency mechanism is necessary.⁷²

Capacity (people), capability (skills) and service excellence (including budget)

As governments strive to implement a BO and PEP disclosure mechanism, the capacity and capability of the people involved in the implementation process should be assessed. The Inter-Departmental Task Force plays a vital role in conducting an audit of the available resources and comparing them to the requirements for managing and implementing the strategy and action plan across the government. This audit should assess the current people capacity and skills in place and identify any additional skills required to implement the BO and PEP transparency mechanism.

The human resource requirements should be costed, along with the operational costs, to implement the strategy. A full zero-based budget plan over the medium term must be developed to implement the cabinet-approved/mandated strategy in a phased and affordable manner. It is unrealistic to expect that a strategy of this nature can be accommodated within existing budgets. Therefore, budgeting for the BO and PEP transparency mechanism is necessary.

Officials in the Inter-Departmental Task Force should leverage existing resources and work collaboratively with civil society, international organizations such as the OECD, UNODC, World Bank, FATF, and others, as well as donors that provide technical assistance and capacity

⁷² There are economic benefits to implementing BOT and PEP scrutiny measures, that could improve revenue collections and prevent base erosion and profit shifting, but that these will likely accrue elsewhere (compared to where the expenses are. For further information, see: <https://www.openownership.org/en/publications/measuring-the-economic-impact-of-beneficial-ownership-transparency-summary-report/>

building, to address any shortfalls. All avenues should be explored to create a BO and PEP transparency centre of excellence. Doing so creates long-term benefits by preventing money from illicitly or illegally leaking from the domestic economy, thereby increasing the pool of resources available for local economic growth.

Consider the following:

- What skills and specialists are required?
 - management and administrative staff;
 - technical staff (policy and legal specialists, economists, AML/CFT and corruption experts);
 - ICT experts including ICT architects or business process engineers, software and hardware engineers, cyber-security and data security specialists;
 - data analysts, big data specialists; AI and ML and Social Network Analysis experts;
 - investigators and case managers;
 - monitoring, reporting and compliance experts; and
 - communications expert (digital, video, social media and traditional media experts).
- What should be budgeted for?
 - line items for hardware and software;
 - tools of the trade and communication materials; and
 - training and capacity building.
- What are the medium-term budget implications?
- How can existing resources be leveraged, adapted or pooled together to meet the objectives of the national strategy for a BO and PEP transparency mechanism?
- What alternate funding sources and technical assistance can be brought in to meet the desired outcomes and objectives?

Training and capacity building

To successfully implement a BO and PEP transparency mechanism, it is essential to provide personnel with the necessary training and capacity building. This training should be differentiated for the various stakeholders involved in the mechanism, including beneficial owners, financial institutions, DNFBPs, and officials who need to track, trace, or match transactions and analyse data.

The training should cover the entire value chain of the mechanism, from reporting requirements to data analysis and investigation. It should be kept relevant to ensure that personnel are equipped with the necessary skills and knowledge to implement the mechanism effectively. Online training and webinars should be explored to ensure that training is accessible to all stakeholders and is cost-effective. In addition, it is important to have tailored training for specific cases.

Capacity building is also crucial to ensure that personnel have the necessary skills and knowledge to implement the mechanism effectively. It should be tailored to the specific needs of each stakeholder group and should be ongoing to ensure that personnel are equipped with the latest skills and knowledge. This includes training on data protection and privacy, risk assessment, and compliance with relevant laws and regulations.

Moreover, capacity building should be integrated into the overall strategy for implementing the BO and PEP transparency mechanism. This includes establishing clear goals and objectives for capacity building, identifying the resources needed, and monitoring and evaluating the effectiveness of capacity building efforts.

Communication and collaboration: stakeholder engagement framework

Effective stakeholder engagement is essential to the implementation process. Communication, collaboration, and sharing of information are integral components of the stakeholder engagement framework. It is crucial to establish clear channels of communication to ensure that all stakeholders are informed and involved throughout the implementation process.

Collaboration among stakeholders, including government agencies, financial institutions, DNFBPs, beneficial owners, and international organizations, is vital to address any challenges and ensure a coordinated approach to implementing the transparency mechanism. By fostering collaboration, stakeholders can share best practices, insights, and resources, ultimately contributing to the effectiveness of the mechanism.

Furthermore, the sharing of information among stakeholders is paramount to enhance transparency and facilitate the smooth operation of the mechanism. This includes sharing relevant data, insights, and feedback to improve the overall implementation process and address any emerging issues.

Innovation in communication strategies can help raise awareness and understanding of BO and PEP transparency principles among stakeholders. Utilizing modern communication channels, interactive tools, and engaging content can improve the dissemination of information and promote compliance with transparency requirements.⁷³

Advocacy and awareness-raising

Advocacy and awareness-raising play a crucial role in the successful implementation of a BO and PEP transparency strategy and mechanism. Effective communication is essential to ensure that stakeholders understand their roles and responsibilities and are able to comply with the requirements in a clear and accessible manner.

Differentiated communication tailored to specific user groups is essential for effective advocacy and awareness-raising. This includes internal communication for the Inter-Departmental Task force, supervisory or regulatory authorities, and government entities. The use of real-life examples,

⁷³ *Op. cit.*, FATF (2023b).

typologies, and actual cases can enhance understanding and facilitate learning among these user groups.

Quasi-external communication is also important for engaging with financial institutions, DNFBPs, and other relevant institutions required to comply with BO and PEP transparency, disclosure, and oversight. Clear and targeted communication can help these entities understand their obligations and facilitate compliance.

External communication with the public is equally vital, particularly in relation to BO and PEP disclosure requirements. Utilizing tools such as Frequently Asked Questions, infographics, short video tutorials for electronic form completion, and ChatBots for basic inquiries can simplify the compliance process and promote understanding among the public.

Social media platforms such as websites, Facebook, and X (formerly Twitter) can be utilized to reach a broad audience. Information should be presented in plain language and supplemented with visual aids such as images, videos, and infographics to enhance awareness and advocacy on BO and PEP transparency, ML and TF risks, corruption, and bribery.

Information sharing requirements

Simplified strategies within a country's borders involve the establishment of MOA or MOU to facilitate the exchange of information. Ideally, real-time information exchanges with direct, secure live links to various databases are preferred. Some of these intricate processes should be integrated into the national strategy and entrusted to an Inter-Departmental Task Force to facilitate information exchange among governments, financial institutions, DNFBPs, and other relevant entities.

Similarly, it is imperative to establish MOA or MOU delineating the terms and conditions of collaboration and information exchange between government and private sector institutions in foreign jurisdictions. This should also be integrated into the national strategy, with the Inter-Departmental Task Force establishing sub-committees or smaller working groups to engage and mutually support counterparts in other jurisdictions.

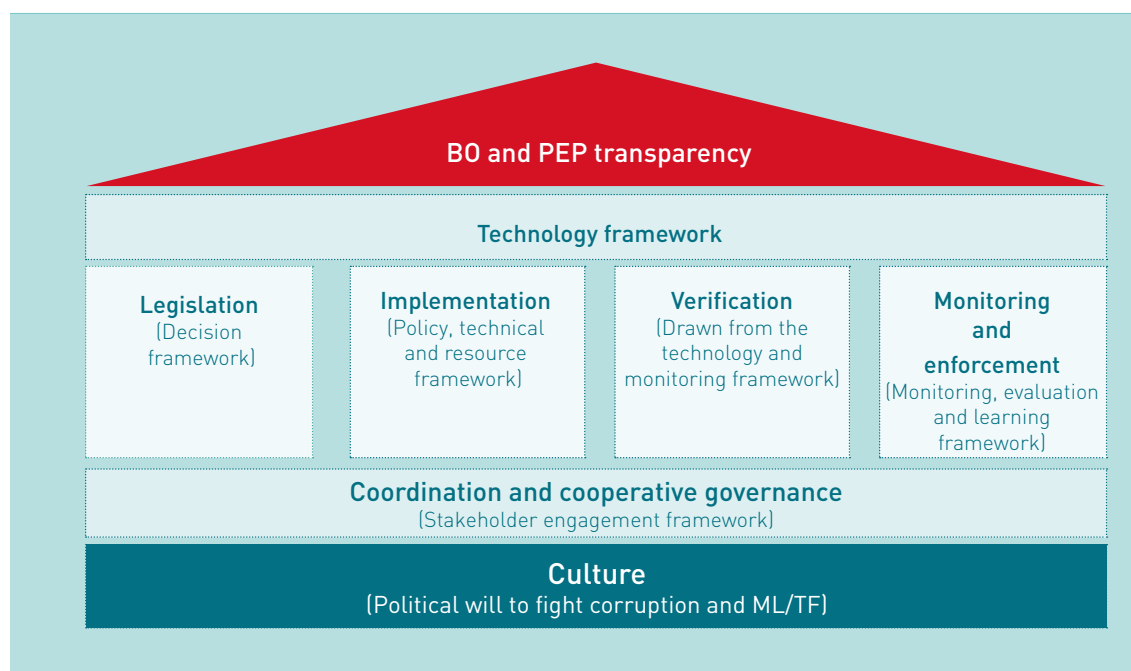
Bringing the 7 pillars together

The toolkit therefore encapsulates a range of policy and legal systems, strategy, skills and collaboration efforts, as well as data and technology characteristics for an effective disclosure regime that supports the achievement of policy goals that promote BO and PEP transparency in order to tackle ML and TF, reduce corruption and IFFs, while increasing domestic resources for the local economy, promoting economic growth and development. It also highlights the various

steps in the value chain necessary to build a comprehensive, integrated BOT and PEP scrutiny mechanism.

Figure 17 threads all the elements of the toolkit into a single graphic highlighting the various pillars and elements as well as the cross-cutting strategic role of government, the tactical role of the supervisory and regulatory authorities and the operational role of financial intermediaries.

Figure 17: Seven areas of action to implement an effective BOT and PEP transparency framework



The following complementary recommendations are also essential:

- **Public sector reform:** This is required to increase: transparency and accountability; efficiency and effectiveness; fairness and equity; restores trust to prevent a defensive attitude.
- **Administrative simplification of processes:** avoid unnecessary administrative burdens; put measure in place to facilitate compliance; increase the ease and ability to comply; increase service provided by relevant agencies to improve intrinsic motivation to comply.
- **Performance management in the public sector:** promote merit-based appraisal systems; enhances transparent and attractive performance evaluation; encourages performance-based incentive (e.g., performance-based pay, performance-based postings);⁷⁴ results in efficient internal controls; and promotes goal-congruence in public sectors (government officials and government sharing values or goals); and publish key performance indicators to demonstrate the benefits of BO transparency.
- **Staff rotation as a precautionary measure:** to prevent public officials from developing long-term relationships with public sectors that would undermine the integrity, impartiality, and quality of the public service; reduce the risk of power abuse; reduce job

74 About performance-based posting, see Khan, Adnan Q., Asim Ijaz Khwaja, and Benjamin A. Olken. 2019. „Making Moves Matter: Experimental Evidence on Incentivizing Bureaucrats through Performance-Based Postings.“ *American Economic Review*, 109 (1): pp. 237–70.

monotony; reduce the incentive for unethical behaviour; and improve the work culture.

- **Improve public scrutiny:** raise awareness; ensure that public powers are used in line with the law; amplify the voice and concerns of the public; and promote oversight from the CSOs and the public.
- **Strengthen and improve the relationship between citizens and the state:** increase mutual trust, transparency, and reliability; encourage civil participation; and incorporate citizens needs into the decision-making process.
- **Build social norms to complement rules and regulations:** the enhancement of workplace values and a Code of Conduct; name and shame wrong doings; respect for the rule of law; promote high standards of ethical behaviour; import norms to the most “influential” individuals first, accelerate the diffusion in their networks and maximize the influence; promote advocacy from CSOs; encourage pressure from the media or investigative journalism
- **Raise awareness of the benefits of BO and PEP transparency and disclosure:** highlight the benefits for governments to combat financial crime and help economic growth; showcase the benefits for private sectors, especially Micro, Small, and Medium Enterprises (MSMEs) who did not have resources to verify the reliability of their business partners, creating trust in the business environment; highlight the benefits for ordinary citizens, creating more trust in government, and a more open and competitive environment for the society.





Recommendations and conclusions

Recommendations

This toolkit has considered several policy frameworks and initiatives influencing BO and its objectives in Southern Africa, outlining the various thrusts, progresses, limitations and opportunities for the development of BO in Southern Africa and examining the work and role of FATF and the Global Forum, Exchange of Information, the Open Government Partnership, the Extractives Industry Transparency Initiative, BO as anti-abuse measures in Double Taxation Agreements and the threat of derisking. Its objectives were to understand and present the existing policy space for BO in Southern Africa to enable stakeholders advocating for BO to better do so. In support of the overall conclusions and recommendations,⁷⁵ this toolkit notes and recommends the following:

- Legislative reforms are necessary to promote a holistic and effective BO and PEP transparency mechanism.
- A national strategy should be developed with clear action plans to implement a holistic and effective BO and PEP transparency mechanism, which should be supported at the highest level. The national strategy and action plan should establish an Inter-Departmental Task Team or Task Force to ensure that the strategy is implemented, coordinating the tasks across a multitude of role players. This should be complemented by an effective communications strategy – internal, quasi-external and external.
- To implement a central (public) registry for BOT, the company approach should also link up to legal arrangements such as trusts, the registry approach, and the existing information approach. The central register ought to:
 - include PEP information;
 - interface with the PEP registry;
 - interface with the Trust registry that should have information on the beneficial owners; and
 - interface with the public procurement registers that gather BO information.
- Implement a separate PEP registry.
- Implement a Trust registry.
- The technical strategy should include a series of policy levers to complement BO and PEP transparency, including:
 - AML/CFT strategies drawing on FATF's 40+ recommendations;
 - Anti-Corruption (and UNCAC);
 - Asset confiscation, recovery and forfeiture;
 - Exchange of information reporting;
 - Country-by-country reporting;
 - Tax and customs investigations;
 - Voluntary tax disclosure programmes;
 - UWOs;
 - Illicit enrichment;
 - Asset declarations by PEPs; and
 - Open government contracting and public procurement.

75 R. Jalipa and E. Danzi (2020). Tax Justice Network Africa: The Case for Beneficial Ownership A Discussion Paper on the policy frameworks promoting Beneficial Ownership in Africa, August 2020: pp. 38–39.

- Support AML/CFT efforts including addressing deficiencies related to risk assessment and creating procedures to ensure that companies cooperate with authorities in the determination of the BO through FATF Recommendation 24.
- To go beyond the FATF recommendations on BO, including requiring BO information from all legal entities and arrangements, including trusts and private foundations, not just legal vehicles such as companies and to make BO information up-to-date, verified and verifiable by making it publicly available, accessible and adequate for BO purposes (including disallowing bearer shares and nominees), enforced through sanctions.
- To take advantage of the exchange of Information (preferably automatic) by engaging with the Global Forum on Transparency and Exchange of Information for Tax Purposes by becoming members and contributing to its working groups and making exchange of Information requests and through the Africa Initiative to benefit from technical assistance in order to be able to use increased transparency to identify income and assets on which tax is evaded.
- Collect BO and PEP disclosure information through electronic means, while using data standards (such as BODS) that render BO and PEP data interoperable, across government, the private sector, civil society in the domestic economy and across the globe.
- Update and verify information regularly, ensuring that the information is relevant, accurate and up-to-date, real-time. This includes addressing the maintenance of historical data.
- Trace ownership information across multiple entities and jurisdictions by using unique identifiers so that transactions, entities and natural persons can be matched unambiguously. The use of LEIs can significantly improve transaction matching to entities across multiple and the LEI code includes a flag for indicating the existence of a relationship, ensuring that any transaction can be examined accurately from source to destination. Promoting global adoption of such a unique identifier will significantly improve the analysis of BO, while reducing the cost of compliance.
- Develop a system to examine cross-border capital flows in areas such as financing for development projects especially for cross-border infrastructure financing arrangements between a state-backed lender and receiver.
- Support financial intermediaries on their roles to promote BO and PEP transparency including providing more direction to professional bodies such as lawyers, bankers and accounting associations on their duties to the public.
- To participate in the regulation of de-risking by disabling local bank secrecy laws, investing in data monitoring including through BO registers, promoting the sharing of information between FIs and enforcing the implementation of KYC rules.
- Promote the global framework for enabling data exchange, cross-referencing, tracing and analysing BO and PEP data across multiple entities and foreign jurisdiction.
- Use technologies such as DLTs, digital identity, big data analytics, algorithms, AI and ML, social network analyses and chain analyses to improve the tracking, tracing and analysing the opaque relationships between entities and the ultimate beneficial owner, rendering this more accessible and shareable while reducing the cost of compliance and invasive surveillance across jurisdictions. The DLT is already being considered by financial institutions for digital ID and SSI (identity wallets), trade digitization, cross-border payments, remittances and even for settlement infrastructure.

Conclusions

The concealment of BO is a significant vulnerability for ML activity worldwide, and it continues to pose a major challenge to the FATF and Egmont communities. The globalization of commerce, trade, and financial and professional services, as well as increased access to opaque legal vehicles, are all enduring challenges that will affect the availability of information on the beneficial owner. There is no one solution to this problem, and the global endeavour to enhance transparency will require numerous iterative and interrelated solutions, and the continued will of governments, private organizations, and the public to implement them.

In recent years, there has been significant progress in counteracting all forms of IFFs, ML, TF, tax evasion and corruption, reflecting a new political focus on the ways these flows undermine the revenue base and therefore the sovereignty and integrity of democracies. The emphasis has now shifted away from developing new standards to implementing the existing standards more effectively. However, effective implementation of the standards is lacking, limiting the ability of international organizations to evaluate the weaknesses or strengths of the standards.

Since 2012, many countries have made progressive efforts to put in place a more robust legal framework to prevent legal entities and arrangements from being misused. With the flexibility provided by the FATF recommendations in implementing R.24 and achieving IO.5, countries are exploring different measures to ensure the transparency of BO. It is expected that countries will continue to improve their system, particularly in relation to the requirements to ensure that adequate, accurate, and up-to-date basic and BO information is available to the authorities in a timely manner.

Under a multi-pronged approach, it is vital to effectively monitor key gatekeepers for compliance with their CDD and ECDD obligations and enforce those requirements, including identifying and shutting down those who facilitate misuse of corporate structures. It is also expected that countries will take action to facilitate the timely sharing of basic and BO information at the domestic and international level to address barriers to information-sharing.

In Southern Africa, several policy frameworks and initiatives are influencing BO and its objectives. Legislative reforms are necessary to promote a holistic and effective BO and PEP transparency mechanism in each country on the continent. A national strategy should be developed with clear action plans to implement a holistic and effective BO and PEP transparency mechanism, which should be supported at the highest levels. The national strategy and action plan should establish an Inter-Departmental Task Team to ensure that the strategy is implemented, coordinating the tasks across a multitude of role players. This should be complemented by an effective communications strategy – internal, quasi-external, and external.

This step-by-step practical toolkit is a valuable resource for governments seeking to implement BOT and PEP scrutiny principles. The toolkit is designed to increase knowledge and awareness of international good practices that have been developed by a growing number of countries around the world in implementing BOT and PEP scrutiny principles. It is intended to be a comprehensive guide that can be used by government agencies, LEAs, corporate registries, trust

registries, FIUs/FICs and anti-corruption agencies or secretariats, to navigate the journey from considering BOT to publishing data on beneficial owners in a central (public) register. It is divided into seven focal areas, so it can be implemented according to the stage a specific jurisdiction is in, in their implementation journey, regardless of whether the country government is considering the options, working to render an existing BO register public, or establishing a new register. This means that the toolkit can be used by countries that are considering the options, working to render an existing BO register public, or establishing a new register.

It is important to note that there is no one-size-fits-all approach to BOT and PEP scrutiny. This toolkit is designed to help jurisdictions design and implement policies and systems that work within specific country contexts and can bring about intended policy impact. BOT is a relatively new policy area, and best practices are still emerging. Therefore, this toolkit should be understood as a work in progress that will continue to evolve and improve over time in response to ongoing collaborations with governments around the world.

In conclusion, this toolkit is a valuable resource for governments seeking to implement BOT and PEP scrutiny principles. By providing practical guidance and resources for each focal area, it can help jurisdictions design and implement policies and systems that work within specific country contexts and bring about intended policy impact.

REFERENCES

- BEIS. (2019). Review of the implementation of the PSC Register. *BEIS Research Paper Number 2019/005*.
- Betti, S., Kozin, V. and J-P. Brun (2022). *Orders without Borders: Direct Enforcement of Foreign Restraint and Confiscation Decisions*. StAR, World Bank Group. Available at https://star.worldbank.org/sites/default/files/2021-12/Orders%20without%20Borders_final.pdf.
- Bosisio, A., Carbone, C., Jofre, M., Riccardi, M., & Guastamacchia, S. (2021). *Developing a Tool to Assess Corruption Risk factors in firms' Ownership Structures – Final report of the DATACROS Project*.
- Brun, J.-P., Gomez, A., Julien, R., Ndubai, J., Owens, J., Rao, S., & Soto, Y. (2022). Taxing Crime: A Whole-of-Government Approach to Fighting Corruption, Money Laundering, and Tax Crimes. In *Taxing Crime: A Whole-of-Government Approach to Fighting Corruption, Money Laundering, and Tax Crimes*. <https://doi.org/10.1596/978-1-4648-1873-8>
- Creme Global (n.d.). *What is a Data Trust?* The Complete Guide for organisations, regulators and manufacturers. Available at *What is a Data Trust?* The complete guide for organizations, regulators and manufacturers. Creme Global <https://www.cremeglobal.com/what-is-a-data-trust-the-complete-guide-for-organizations-regulators-and-manufacturers/>
- Chakravarti, A., (2020). Trumpworld's Corruption Is as Globalized as the Ultra-Rich the President Mingles with Elliott Broidy and others are connected to globe-spanning scandals. <https://foreignpolicy.com/2020/10/12/trumpworld-corruption-elliott-broidy-ultra-rich/>
- Dmytro, K., & Pop, L. (2021). *Automated Risk Analysis of Asset and Interest Declarations of Public Officials A Technical Guide*. <https://star.worldbank.org/publications/automated-risk-analysis-asset-and-interest-declarations-public-officials>
- Eavani, F., Nazari, K., & Emami, M. (2012). Social audit: From theory to practice. *Journal of Applied Sciences Research*, 8, pp. 1174–1179.
- FATF (2011). *Laundering the Proceeds of Corruption*. <https://www.fatf-gafi.org/media/fatf/documents/reports/Laundering%20the%20Proceeds%20of%20Corruption.pdf>
- FATF. (2014). *Guidance on Transparency and Beneficial Ownership*.
- FATF (2020), *Guidance on Digital Identity*, FATF, Paris, www.fatf-gafi.org/publications/documents/digital-identity-guidance.html
- FATF. (2023a). *Guidance on Beneficial Ownership for Legal Persons*.
- FATF. (2023b). *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*. [FATF. %0Awww.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html](http://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html)
- FICAM (n.d.). Streamline Identity Management Playbook. United States Federal Identity, Credential, and Access Management. Available at: https://bnbuckler.github.io/ficam-identity/2_step-2/
- Fonzetti Colladon, A. and E. Remondi (2017). Using Social Network Analysis to Prevent Money Laundering. *Elsevier Expert Systems with Applications*, vol 67, January 2017, pp. 49–58. Available at <https://doi.org/10.1016/j.eswa.2016.09.029>
- Global Witness. (2018). *The Companies We Keep: What the UK's open data register actually tells us about company ownership*.
- Goodley, S., Harding, L., Mason, R., & Davies, H. (2021). Revealed: how Tory co-chair's offshore film company indirectly benefited from £121k tax credits. *The Guardian*.
- Goodley, S., & Smith, J. (2021). Revealed: Pandora papers unmask owners of offshore-held UK property worth £4bn. *The Guardian*.
- Hedera Hashgraph. (n.d.). *What are distributed ledger technologies?* | Hedera Hashgraph. Available at: https://hedera.com/learning/what-are-distributed-ledger-technologies-dlts?gclid=CjwKCAiAkJKCBhAyEiwAKQBCKq4o3TUZz0AC7pvgeW2dt-og4oiw4zQjcQ_vJ_9fUMne61-MjFby3BoCoTMQAvD_BwE, accessed 18 February 2021.
- Harbitz, M. and K. Kentala. (2013). *Dictionary for Civil Registration and Identification*. Washington, DC: Inter-American Development Bank. Available at: <https://publications.iadb.org/en/dictionary-civil-registration-and-identification>
- ID4D (2016). *Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation*, A joint World Bank Group–GSMA–Secure Identity Alliance Discussion Paper. Available at <http://documents.worldbank.org/curated/en/600821469220400272/Digital-identity-towards-shared-principles-for-public-and-private-sector-cooperation>
- ITPRO (2020). *What are data trusts and how do they work?* Available at: <https://www.itpro.com/in-depth/354740/what-are-data-trusts-and-how-do-they-work>
- Khan, Adnan Q., Asim Ijaz Khwaja, and Benjamin A. Olken. 2019. “Making Moves Matter: Experimental Evidence on Incentivizing Bureaucrats through Performance-Based Postings.” *American Economic Review*, 109 (1): pp. 237–70.

- Kotlyar, D, and L. Pop. (2019). E-filing Asset Declarations: Benefits and Challenges. World Bank, Washington, DC. <http://hdl.handle.net/10986/32066> License: CC BY 3.0 IGO.
- Laney (2001). Others have expanded on this definition adding other attributes (while keeping to the V theme), including variability, validity, value, and veracity, among others (NIST Big Data Public Working Group, 2015a, p. 7).
- Malinga, S (2018). "ABSA joins Sovrin Foundation in blockchain, security push", ITWeb Business Technology Media Company, 16 August, 2018, <https://www.itweb.co.za/content/Kjlyr7wdjPQMk6am>, accessed 14 December, 2020.
- Nicolaou-Manias, K., & Wu, Y. (2022). *Toolkit for Beneficial Ownership and PEP Transparency. Tax Notes International*. 106(2), pp. 205–220.
- NIST. 2017. SP 800-63:2017 *Digital Identity Guidelines*. Available at <https://pages.nist.gov/800-63-3/>.
- Open Ownership (2023). The Open Ownership Principles for Effective Beneficial Ownership Disclosure. January 2023. Available at: [oo-guidance-open-ownership-principles-2023-01.pdf](https://openownership.org/publications/oo-guidance-open-ownership-principles-2023-01.pdf) (cdn.ngo)
- Panico, Paolo. "Private Foundations and EU beneficial ownership registers: towards full disclosure to the general public?." *Trusts & Trustees* 26, no. 6 (2020): 493-502.
- Sharman, J. (2009). Regional Seminar on Political Economy of Corruption: Politically Exposed Persons (PEPs). Griffith University, Australia, 9 September 2009, ADB Headquarters, Manila, Philippines. ADB/OECD Anti-Corruption Initiative for Asia and the Pacific. [Oecd.org](https://www.oecd.org/site/adboecdanti-corruptioninitiative/meetingsandconferences/44442190.pdf). Available at: <https://www.oecd.org/site/adboecdanti-corruptioninitiative/meetingsandconferences/44442190.pdf>, accessed 8 January 2021.
- Transcrime. (2018). *Mapping the Risk of Serious and Organised Crime Infiltration in Europe - Final Report of the MORE Project*.
- UNCTAD (2023). *Economic Development in Africa Report 2023*. Available at <https://unctad.org/publication/economic-development-africa-report-2023>
- UNODC. (2021). Organized crime strategy toolkit for developing high-impact strategies.
- White, J. (2021). OpenLux shows failures of beneficial ownership registers. *International Tax Review*.
- World Bank. (2022). Legal Persons and Arrangements ML Risk Assessment Tool: With guidance on assessing risks related to beneficial ownership transparency.
- World Bank (2016). Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation. A Joint World Bank Group – GSMA – Secure Identity Alliance Discussion Paper. [online] Available at <http://documents1.worldbank.org/curated/en/600821469220400272/pdf/107201-WP-PUBLIC-WB-GSMA-SIADigitalIdentity-WEB.pdf>, accessed 17 December 2020.
- Websites:**
- <https://oecd-opsi.org/innovations/e-register-of-asset-declarations-of-public-officials-in-ukraine/>
- Open Ownership (2021), <http://standard.openownership.org/en/latest/schema/index.html>, accessed 21 January 2021.
- Open Ownership (2021), <http://standard.openownership.org/en/latest/examples/index.html>, accessed 21 January 2021.
- Open Ownership, <https://www.openownership.org/en/publications/measuring-the-economic-impact-of-beneficial-ownership-transparency-summary-report/>
- <https://offshoreleaks.icij.org/nodes/240024734>
- <https://offshoreleaks.icij.org/nodes/240025610>
- <https://offshoreleaks.icij.org/nodes/10144712>
- <https://www.openownership.org/en/publications/beneficial-ownership-declaration-forms-guide-for-regulators-and-designers/>
- <https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/a-kyc-aml-utility-driving-scale-efficiency-and-effectiveness>
- <https://www.identity.com/self-sovereign-identity/>
- https://www.taxjustice.net/2020/10/08/how-denmark-is-verifying-beneficial-ownership-information/?fbclid=IwARITPpzwJNB1q0ehduSpucx5y1B2U1q62gT1e5_MGfCEoJn6k572MBW_AE
- <https://gfmag.com/features/de-risking-technology-aml/#:~:text=Fixing%20AML%3A%20Can%20New%20Technology,solve%20the%20de%2Drisking%20problem>
- <https://www.taxjustice.net/2019/09/06/more-beneficial-ownership-loopholes-to-plug-circular-ownership-control-with-little-ownership-and-companies-as-parties-to-the-trust/>
- <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/R25-public-consultation.html#:~:text=%E2%80%9CBeneficial%20owner%20refers%20to%20the,a%20legal%20person%20or%20arrangement>



UNODC

United Nations Office on Drugs and Crime