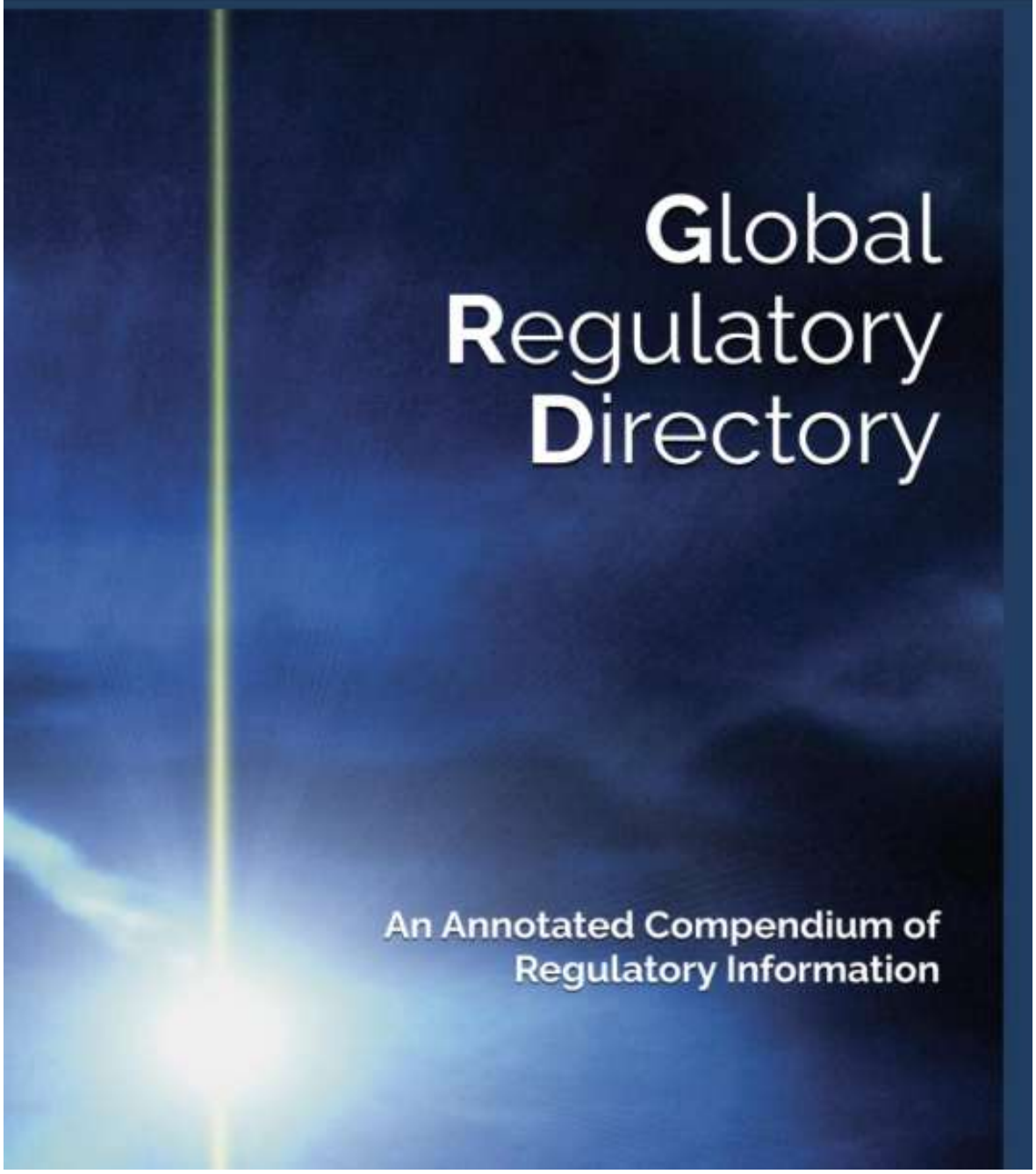
kyc-data.com



Global Regulatory Directory

An Annotated Compendium of Regulatory Information

ISBN-13 : 979-8282366907

Global Regulatory Directory

An Annotated Compendium of Regulatory Information

May 2025

Copyright Notice

Issue 1 - May 25th, 2025

Published by EAMindset (UK) Ltd

Table of Contents

Table of Figures

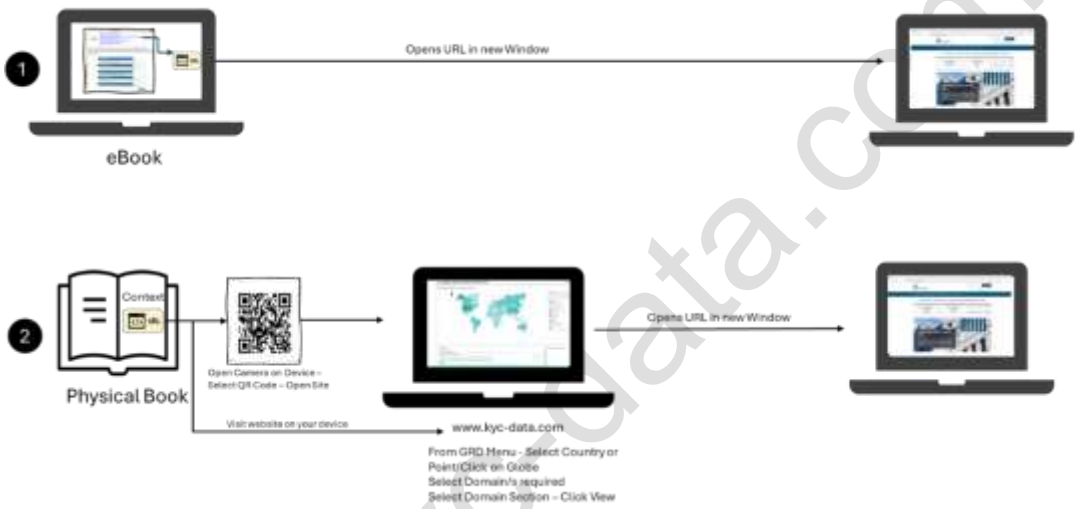
How to Use the Deskside Directory

The Global Regulatory Directory (**GRD**) delivers a standalone **deskside resource** providing an additional layer of context for material found at the GRD section of the www.kyc-data.com portal.

The GRD is distributed in two versions:

1. The **e-Book,** which is recommended and provides additional URLs not found at www.kyc-data.com provides value in relation to analysis of meta data available.
2. The **printed version** is for those who prefer to read a hardcopy of the publication.

The illustration below highlights a typical usage scenario for each version of the GRD.



If reading this e-Book on your device the URLs, when selected, will be opened in a new window.

If you are reading the printed version, you can use the following QR code (quick-response code) to visit the kyc-data.com site, where in the GRD window view you can access URLs found in this publication, which are checked for integrity and updated regularly.

In principle the GRD is a guide to the available compliance information, relating to regulatory statutes found in given countries with additional context provided by our analysts at the time of writing.

We have also integrated information, where available, relating to **cloud** and **AI** polices. These domains are emerging and an essential insight for those designing global information systems and require data privacy information.

The GRD provides general information and meta data[1] about each country's domains, along with a summary of the countries posture for the domains shown in Figure 1 below.

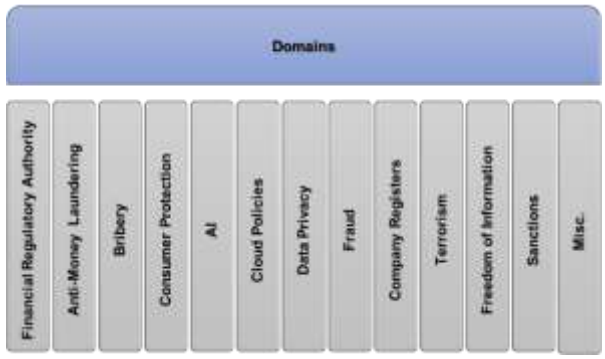


Figure 1 Regulatory Domains

In line with the GRD's classification schema and to enhance visibility, we have associated a color throughout this book for each domain, allowing for a unified simplified classification process illustrated in the table below with a brief description of the domain:

Domain	Overview
Financial Regulatory Authority	The authority or agency which is responsible for the management of the banking sector, regulating additional financial services and other specific monetary matters in the public interest or the government of the day. In most cases the services of the authority are delivered via government departments. However, on the rare occasion where there is a single authority, this will be highlighted. The authority, in most cases, is a central bank and often known as the Reserve Bank, or Monetary Authority which acts as the institution responsible for managing the currency in circulation and the monetary policy of the country or Monetary Union. Additional currency data is provided in the appendices.
Artificial Intelligence (AI) Act / Policy	Artificial Intelligence (**AI**) refers to a set of technologies that enable Information Systems to perform cognitive functions usually associated with humans. AI systems based on machine learning (ML), with the increasing sophistication of generative AI, produce various types of content, including text, imagery, audio and synthetic data all of which can impact elements of privacy and intellectual property. Governments are introducing legislation and policies to support the control and introduction of AI into society, which is captured in the GRD.
Anti-Money Laundering (AML)	AML refers to the processes and practices implemented to prevent and restrict money laundering in a country. Money Laundering is the concealment of the illegal origins of income resulting from criminal activities. Through money laundering, a criminal can transform monetary proceeds, derived from criminal endeavours, into funds with a seemingly legal source.

[1] The metadata we refer to is information provided regarding the URLs in terms of **context** and **location**.

Domain	Overview
Bribery	Bribery refers to the offering, giving, soliciting, or receiving of any *item of value* as a means of influencing the behaviours or actions of an individual holding a public office or specific legal duty. Every country has a set of laws, policies and practices to prevent bribery, which are highlighted in the GRD.
Consumer Protection	Consumer Protection is a selection of laws which protect individual consumers against the unfair selling practices of goods, services and or digital content. Due to the widespread global use of credit cards as a payment method, laws and regulatory notices have emerged to protect consumers from unfair practices by credit card issuers. These laws require greater transparency in credit card terms and conditions and they impose limits on charges and interest rates associated with credit card transactions.
Cloud Policy	Cloud Policy refers to the set of laws, rules and practices for the use of Cloud Computing. Cloud Computing provides data centre capabilities from 3rd parties. These 3rd party service providers usually offer a globally dispersed infrastructure where data is often replicated or stored in multiple geo-locations. The protection and localization of data is an important topic for regulators resulting in policies being promoted by country regulators to address possible breaches of privacy.
Data Privacy	Data Privacy refers to the protection and control of sensitive personal data and the ability for an individual to control how it is used and shared. Examples of personal data may include, but not limited to, financial, health or legal information. Data Privacy laws ensure that information controlled and only accessed by authorized personnel or organizations.
Fraud	Fraud refers to wrongful or criminal deception intended to result in financial or personal gain. Examples include fraud by false representation, failure to disclose information when there is a legal obligation to disclose and abuse of position.
Sanctions	Sanctions represent a mandate from a government or an international body to restrict commerce and official interaction with a person, business or country that has violated its laws. There are different types of sanctions, *economic*, *international*, *embargo* and *diplomatic* sanctions. Sanctions aim to exert pressure on countries. For country specific information please visit the sanctions section of www.kyc-data.com.
Terrorism	Terrorism involves the planning or execution of harmful acts against the state, an organization or individuals to achieve a desired outcome or promote a political, economic or social change. Due to the nature of these acts, countries will specify individuals, groups or organizations involved in terrorism activity which could include those who: • Those who commit or participate in acts of terrorism. • Those who prepare for acts of terrorism. • Those who promote or encourage terrorism (including the unlawful glorification).
Company Registrar	The agency, government department or organization responsible for the registration, compliance and reporting of company information.

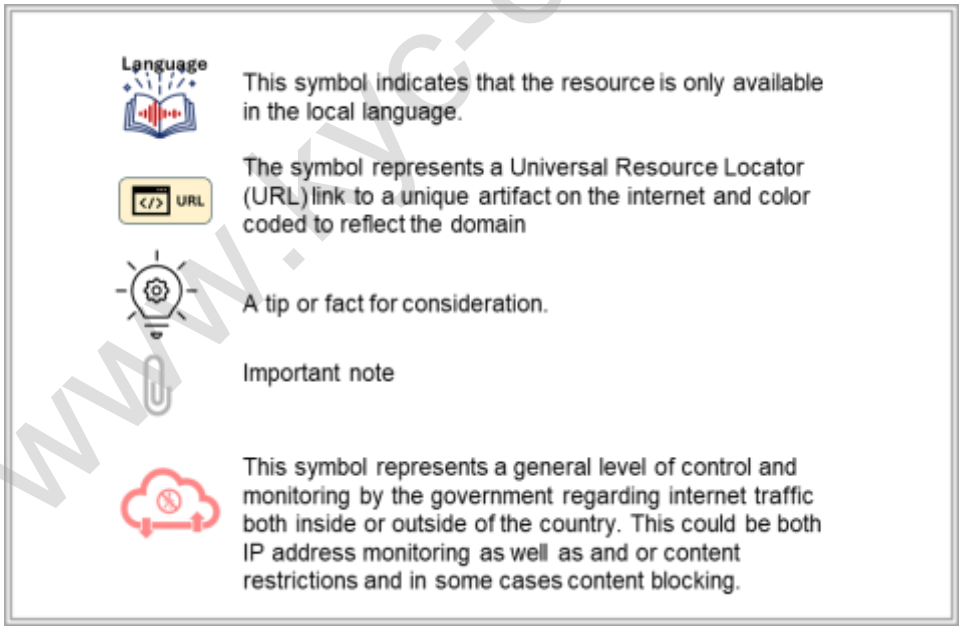
	Domain	Overview
		It is common for countries to allow members of the public to perform queries to find company information and associated tools which are provided in the GRD i.e. the link to the search capabilities.
	Access to Public Information	Many countries allow citizens to access information on various topics and a link is provided in the GRD with context to the countries 'Freedom of Information' laws or policies if available.
	Other	The report highlights any additional compliance information where relevant and any links that pertain to the country; as a default we list the official government website and any information and legislations of potential value.

Posture Rating (PR)	The Posture Rating (**PR**) is an assigned *notional* value derived during country analysis and in the range of 1 to 10 for each domain. This value provides a cursory reflection for the quality and availability of information, together with any processes and tools available to support the domains. Due to the dynamic and rapidly evolving nature of AI and Cloud Policy, these domains have been excluded from the PR value. See Appendices for detailed discussion on how the PR is derived.

If a country presents the information for multiple domains, we will aggregate

Symbols

Below are the key symbols used in this publication:



Note from the Publisher

This publication is produced to allow those working in the Global Regulatory Compliance field to access information quickly and to benefit from our analysis within our commentary. Our overarching philosophy is rooted in the simple consideration that regulation is more than just a process of records, audit and information retention.

Through the provision and scrutiny of the surrounding context we can conduct in-depth analysis, where language permits. Our modus is focussed on enhancing compliance regulation and surveillance by offering a bespoke product concentrated on direct customer value. Something which we aim to reflect in our work.

The default language for our work is English, however in some jurisdictions the policies and acts are often published in their native language.

We share the URL for the source document and provide context where appropriate.

We maintain a set of current updated links at www.kyc-data.com where we validate URL links daily (via digital pings), thus maintaining a set of valid master links. This book provides a physical copy of the data we maintain, alongside additional context where appropriate.

There are many organizations e.g. the OECD, FATF as well as a host of others which provide a vast source of detailed information. Where appropriate we will provide the relative URLs.

Where a government presents an official title in its website for the country e.g. Kingdom or Republic of, we will respectfully adopt the official name for the country in this publication.

We continue to add to the GDR and any requests for the addition of a specific country may be submitted via our website or contact us directly via email :kyc-data@eamindset.com .

All URLs where validated and passed integrity checking at the time of publishing.

About the Authors

This publication has been compiled by members of EaMindset (UK) Ltd to provide a supplementary support resource for users of the www.kyc-data.com website.

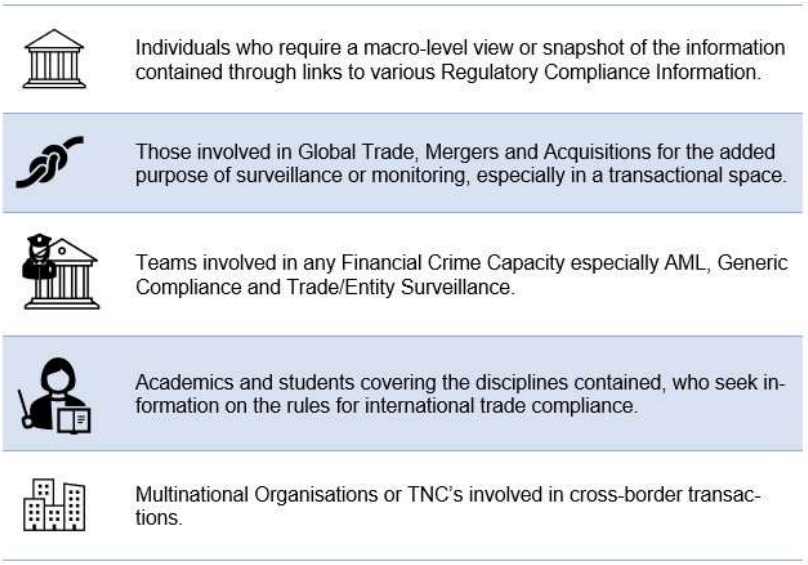
EaMindset is a small specialist European Consultancy with a software development team in Asia. EaMindset has a focus on collecting, creating and disseminating information to allow organizations to meet Global Regulatory Compliance obligations as well as provide bespoke software tools to support the KYC Journey.

.

Who should read this book?

This document is provided as a referential resource for multiple different audiences, with compliance information being directly applied throughout the cross-section of the business, legal and financial communities.

Those who require an understanding of the available resources for a single or collective group of countries. Our resource caters to a diverse range of clientele, which may include the following:



This is a valuable resource for individuals engaged in Global Regulatory Compliance or Business Activities, offering easily accessible links to policy statements and relevant legislation. The information outlined may be used for the purposes of Global Operational Regulatory Governance, Financial Crime, Mergers and Acquisitions, Academic and Teaching, Research and those who require information on the Regulatory Sources for specific countries in a simple format.

Disclaimer

The GRD does not attempt to set out all requirements for the domains listed and should be read in conjunction with existing laws, rules and guidance from the appropriate central government.

If there is a discrepancy between the GRD and any applicable legal requirements, the provisions of the relevant requirement prevail.

If in doubt, please seek appropriate professional advice.

All URLs where validated and passed integrity checking at the time of publishing (24th May 2025).

Argentina

Commentary

Financial Regulatory Authority

https://www.bcra.gob.ar/varios/English_information.asp (i)
https://www.bcra.gob.ar/BCRAyVos/catalogo-de-APIs-banco-central-i.asp (ii)
https://www.argentina.gob.ar/cnv/ (iii)

The Argentine Central Bank (**BCRA**) is the central bank of the Republic of Argentina and currently self-administered and regulates the operation of Argentina's financial system. This body enforces any law on Financial Institutions.

The BCRA is governed by a board consisting of a Governor, a Deputy Governor and eight members.

The BCRA's international Reserves (in million USD) as of 12th May 2025 was **38,258** (i)

Argentina's Central Bank is one of the many few banks that provides a set of application programming interfaces (APIs) for Developers – currently only available in Spanish.

(ii)

National Securities Commission (**NSC**) the body responsible for the regulation, supervision, promotion and development of the Argentinian capital market.

(iii)

The legal tender currency of Argentina is the Argentine **peso**.

AI Act / Policy

https://servicios.infoleg.gob.ar/infolegInternet/anexos/315000-319999/318677/res138.pdf (i)
https://publications.iadb.org/es/prometea-transformando-la-administracion-de-justicia-con-herramientas-de-inteligencia-artificial (ii)

Spanish

Argentina's strategy towards regulating AI is enshrined within **Argentina's Digital Agenda 2030**. This includes promoting AI adoption across different sectors, developing legal frameworks to support its use and ensuring ethical and responsible development.

(i)

The commitment, gains and advancement of AI is best observed by the **Promethea Project**, a pioneering AI tool in the Buenos Aires judicial system (See the IDB Report on Promethea – *Transforming the Administration of Justice with AI Tools*).

(ii)

At the time of writing source documents are only available in Spanish.

Commentary

Anti-Money Laundering

https://www.argentina.gob.ar/uif (i) National Strategy 2022/24

https://www.argentina.gob.ar/sites/default/files/2022/09/estrategia_nacional_para_la_prevencion_y_el_combate_al_lavado_de_activos_la_financiacion_del_terrorismo_y_la_proliferacion_de_armas_de_destruccion_masiva_0.pdf (ii)

Argentina's Financial Information Unit (**FIU**) is a special governmental agency responsible for ensuring compliance with the Anti-Money Laundering Law of Argentina.

The FIU is responsible for analysing, processing and transmitting information with the objective of preventing and deterring money laundering.

Argentina enacted the **Anti-Money Laundering Law No 25246 in April 2000**, a law that defines money laundering as a provocation of an underlying crime.

Argentina also uses prevention policies that are implemented by the USA Patriot Act. There is no relationship with Shell Banks or Entities involved in terrorist activities. It does not render downstream correspondent banking services nor payable-through accounts services.

The AML/CFT policies and procedures apply in all processes to the circuits defined by the Institution to Head Office, Domestic and Foreign Branches and Subsidiaries.

(i)

In 2020, the process of preparing the first National Money Laundering Risk Assessment began. This involved Assets (**ENR-LA**) of the Argentine Republic working with the Bank Inter-American Development Bank (**IDB**). The process concluded in 2022, with the adoption of the report by the AML/CFT/PIC Coordination Committee and subsequent approval by the Chair of the Nation through Decree No. 653/2022.

(ii)

Bribery

https://www.argentina.gob.ar/normativa/nacional/decreto-1179-2016-267949/texto

The legislation of Argentina strictly prohibits any form of bribery; they define this as the promise, offer, giving, acceptance or solicitation of any value, whether financial or not. It includes if the bribe is made indirectly or directly and accepting any bribe is an offence.

Public officials are forbidden from receiving all gifts or donations, although **Decree No. 1,179/2016** and Decree No. 5,013/72 states that *'benefits or gratuities have been received on the occasion of the performance of their duties which they would not have been offered if the recipient did not hold the position which he or she holds, except for gifts of courtesy or diplomatic custom'.*

The corporate criminal liability **Law No. 27401** (March 2nd, 2018) *states that companies are liable for corruption offences***.** Argentina is updating its anti-corruption laws to combat current offences. The law in Argentina does not cover bribery between private parties in a commercial transaction.

Consumer Protection

Argentina Version

https://www.bcra.gob.ar/pdfs/comytexord/A6664.pdf (i)

http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/265949/texact.htm (ii)

Protection of users of financial services regarding:

- communication through media electronics for the care of the environment
- exterior and Changes
- interest rates in credit operations
- all Adequacies

Commentary

In 2016, the AAIP issued a new regulation, Provision 60-E/2016, governing cross-border transfers of personal data. Under the rule, it approved model forms for such transfers to **data controllers and data processors**.

(i)

Law 27,275 defines public information as any *information bound parties may create, obtain, control, transform or keep*. The Law on **Freedom of Information** allows citizens to exercise their right to access public records, thus ensuring transparency in public affairs.

(ii)

Cloud Policy

https://www.bcra.gob.ar/pdfs/comytexord/A6375.pdf

It is important to note that Argentina's laws require internet service providers to provide the Argentinian authorities access to user **data for surveillance**.

The BCRA Comunicacion A 6375 addresses the minimum requirements for the management, implementation and control of risks related to information technology, information systems and related resources for financial entities.

Oracle, Microsoft and IBM are the main International Cloud providers in Argentina, although not all of them have SaaS, IaaS and PaaS as part of their service offering.

Most Argentinian telecommunications companies provide cloud computing capabilities. Local companies providing cloud services include Claro, Movistar and ARSAT (*a government-owned telecommunications company*). The business model is mostly based on providing hosting and offering flexible payment options.

Data Privacy

https://www.argentina.gob.ar/aaip/datospersonales (i)

http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/267922/norma.htm (ii)

The official website of Director of Personal Data Protection (**DPDP**) providing URL links.

(i)

Personal Data Protection Act 25.326 (PDPA) (Ley de Protección de los Datos Personales), aka the "**PDPA**") and then Regulation Decree 1558/2001. Convention 108 and Convention 108+. entered into force on November 2, 2000.

The Argentine Agency of Access to Public Information (Agencia de Acceso a la Información Pública- **AAIP**) within the chief of ministries' cabinet is responsible for enforcing this law.

In 2016, the AAIP issued a new regulation, Provision 60-E/2016, governing cross-border transfers of personal data. Under the rule, it approved model forms for such transfers to data controllers and data processors.

(ii)

Commentary

Fraud

https://www.bcra.gob.ar/noticias/actualizacion-normas-seguridad-prevencion-fraudes-i.asp

The Central Bank of Argentina (**BCRA**) regularly updates the regulations to bolster security and fraud prevention in digital financial services. New standards cover governance, technology risk management, protection measures and service monitoring. This is for digital financial institutions and payment service providers to enhance security in digital financial services.

The BCRA addresses evolving risks through the issued guidelines and regulations, including measures for cyber incident response and recovery (2021), fraud prevention in transfers (2022) and minimum requirements for technology and information security risk management (2023).

The updated regulations now cover digital identification, prevention of identity theft through mobile apps, monitoring client transactions, app and device control, prevention of identity theft through mobile apps and control against fraudulent accounts, apps and websites. The framework's aim is to safeguard uses, ensure financial stability and promote operational resilience.

The guidelines are effective 180 days post-publication and financial institutions have time to align with the new regulations. The BCRA will continue reviewing regulations to adapt to advancements in digital financial services and new payment methods.

Sanctions

https://www.cancilleria.gob.ar/en/foreign-policy/international-security/sanctions-committee (i)

https://www.argentina.gob.ar/uif/sanciones-uif (ii)

According to Article 25 of the UN Charter, members must comply with the Security Council's decisions. In Argentina, Law No. 24,080 and Presidential Decree No. 1521/04 outlines the integration of Chapter VII into decisions in the national legal system. This information is circulated through the Ministry of Foreign Affairs website. (i)

FIU Penalties – A table listing Sanctioning Resolutions for non-compliance with the obligations set forth in Law No. 25,246, its amendments and regulation. (ii)

Terrorism

https://www.argentina.gob.ar/uif

The **FIU,** known as UIF, in Argentina is an autonomous and self-governing body that operates under the Ministry of Justice and is responsible for the analysis, processing and transmission of information for the purposes of preventing and blocking terrorist financing as well as AML.

The FIU is comprised of a President, a Vice-President and an advisory board of seven members comprising of one representative from the bodies as shown in Figure 2 below:

Figure 2 Argentinian FIU Membership

Commentary

Company Registrar

https://www.argentina.gob.ar/justicia/registro-nacional-sociedades/institucional/jurisdicciones

The Public Registry of Commerce in Argentina (**Registro Público de Comercio**) maintains an official company database that provides information on registered companies in Argentina.

Access to Public Information

https://www.bcra.gob.ar/Institucional/Acceso_Informacion_Guia.asp

Law 27,275 on Freedom of Information allows citizens to exercise their right to access public records, promoting their participation and ensuring transparency in public affairs.

Guide to Access Public Information available via the URL.

Other

https://www.argentina.gob.ar/ (i)

https://www.fatf-gafi.org/en/countries/detail/Argentina.html (ii)

Official website of the Argentine State .

(i)

Argentina became a member of the FATF in 2000; Argentina is also an active member of the FATF-Style Regional Boday GAFILAT. Since becoming an FATF member, the country also held the Presidency of the FATF, from 1 July 2017 to 31 June 2018.

(ii)

Posture Rating – Argentina

The PR value of **6.3** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	10	6	6	4	7	6	3	6	6	6	3

Argentina has well-structured and defined processes, regulations and laws to address the domain obligations.

The BCRA is one of a handful of central banks who publish a documented set of public APIs to allow 3rd parties to consume and analyse its information and this is reflected in the PR Value assigned for the Regulatory Authority.

N.B:The figure does not reflect the execution of any processes, laws or regulations

The PR value is assigned subject to the public information available at time of writing.

Armenia

Commentary

Financial Regulatory Authority

https://www.cba.am/EN/SitePages/Default.aspx (i)

https://cabinet.arca.am/en/ (ii)

On April 27, 1993, the Republic of Armenia Law on "The Central Bank of the Republic of Armenia" was adopted and the National Bank was re-named the Central Bank of the Republic of Armenia.

The Central Bank of Armenia Board consists of the Governor of the Central Bank, two Deputy Governors and five Board Members. The Central Bank Governor and Deputy Governors are appointed by the Republic of Armenia National Assembly for a 6-year term. Members of the Central Bank Board cannot hold other positions in the Central Bank.

(i)

When discussing the Financial Composition of Armenia, it is prudent to mention the **ArCa** system introduced by the Armenian commercial banks and the Central Bank in 2001. The owner and operator of the system is 'Armenian Card' CJSC.

The settlements in the system are executed according to the principle of multilateral netting while the final settlement is done via correspondent accounts of participant banks with the Central Bank.

Financial organizations operating in or outside the Republic of Armenia and/or other organizations specialized in banking/payment cards can be members of the ArCa system.

'Armenian Card' CJSC is a MasterCard Europe Member and Processing Centre (Member Service Provider) and Third-Party Processor for VISA, American Express and Diners Club International.

'Armenian Card' CJSC presents service package which gives an opportunity to banks to issue and acquire not only ArCa, but also MasterCard, VISA, American Express and Diners Club International cards using the modern technics, technologies and software of the processing centre. Since 2017, because of cooperation between ArCa and Russian "MIR" payment systems, cardholders of ArCa cards can do transactions in the Russian Federation and cardholders of "MIR" cards can do transactions in the infrastructure of ArCa system

(ii)

The legal currency of Armenia is the **dram.**

	Commentary
AI Act / Policy	https://www.eif.am/eng/ Armenia does not have a specific regulation for the use of artificial intelligence, machine learning, or similar technologies. However, the Ministry of Economy and the Central Bank are responsible for the largest technology business incubators in Armenia. The Enterprise Incubator Foundation (**EIF**) is one of the largest technology business incubators and IT/High Tech development agencies operating in Armenia. They have the following objectives: 1. Develop effective information and communication technology infrastructure to enhance technological advance and transition to knowledge economy 2. Enhance nationwide access to computers and development of e-society 3. Promote Armenian enterprises and increasing their competitiveness in the global markets 4. Create new channels for attracting foreign direct investment to Armenia 5. Build linkages with business and research communities in key technology markets 6. To foster formation of start-ups and their further development; to develop managerial and professional workforce and foster productivity improvement in Armenian companies; and to improve access of local firms to best international practices and experience
Anti-Money Laundering	https://fiu-cis.org/en (i) https://www.cba.am/Storage/EN/FDK/Regulation/AML-CFT%20Law_eng.pdf (ii) The Financial Monitoring Centre (**FMC**) was established in 2005 as a separate unit in the structure of the Central Bank of Armenia. The FMC is an administrative-type financial intelligence unit which acts as an intermediary between reporting entities and law enforcement authorities. The mission of the FMC is to combat money laundering and terrorism financing (AML/CFT. (i) The primary function of the FMC is to *collect, analyse and exchange* information for AML/CFT purposes. Moreover, the FMC represents the Republic in several international organizations and structures, whilst actively participating in international AML/CFT initiatives. The targets and directions of the AML/CFT regime are defined under the National Strategy for Combating Money Laundering and Terrorism Financing. Moreover, the authorities of the FMC are decided under the Republic of Armenia Law on Combating Money Laundering and Terrorism Financing, whilst the organizational structure and functions of the FMC are defined under the FMC Statute. (ii)
Eribery	https://www.gov.am/en/anticorruption-legislation/ (i) https://www.gov.am/files/docs/3518.pdf (ii) Anti-Corruption Legislation regulating the activity of the Council. (i) DECISION 808-N 24th June 2019: Composition of the Anti-Corruption Policy Council. (ii)

	Commentary
Consumer Protection	https://www.cba.am/en/sitepages/fcpintroduction.aspx (i) www.abcfinance.am (ii) https://documents1.worldbank.org/curated/en/411981468207244137/pdf/763440WP0P13020ction0Plan020121204.pdf (iii)
	The **Consumer Rights Protection and Market Conduct Division s**its within the Central Bank of Armenia. (i) The division has several functions, depicted in the illustration below:  *Figure 3 - Armenian CBA Consumer Rights Protection & Market Conduct Division functions* (ii) The action plan on financial consumer protection for Armenia prepared by the World Bank (2012) (iii)
Cloud Policy	https://hightech.gov.am/en/
	The RA Ministry of High-Tech Industry (URL link provided) and Amazon Web Services (AWS) signed a memorandum of understanding in 2023 to modernize the state's technological infrastructure and accelerate the implementation of cloud services in Armenia's public and private sectors.
Data Privacy	https://www.mfa.am/en/priv_pol#:~:text=Processors-,The%20Law%20of%20Armenia%20on%20protection%20of%20personal%20data%20(Data,authorised%20persons%2C%20and%20third%20parties.
	The Constitution of Armenia protects the right to protection of personal data. General rules concerning the processing of personal data are set out in the Law of Armenia on the protection of personal data (Data Protection Law), which was adopted in 2015. See the above URL for the **Confidentiality and Data Protection Policy** of Armenia.
Fraud	http://www.parliament.am/legislation.php?sel=show&ID=1349&lang=eng
	The Criminal Code of the Republic of Armenia.

	Commentary
Sanctions	https://www.cba.am/Storage/EN/FDK/20211021%20-%20National%20Designations%20List_eng.pdf On the 36th Session of the Interagency Committee on Combatting Money Laundering, Terrorism Financing and Proliferation Financing in the Republic of Armenia, held on the 18th of October 2021, they curated the *'LIST OF DESIGNATED PERSONS UNDER THE UNITED NATIONS SECURITY COUNCIL RESOLUTION 1373'.* The list included the assets of individuals and entities subject to immediate freezing (Article 28 of the Republic of Armenia Law on Combating Money Laundering and Terrorism Financing). To initiate the process of delisting designated persons, an application under the UNSC Resolutions is required.
Terrorism	https://www.arlis.am/DocumentView.aspx?docid=128806 The Law of the Republic of Armenia - On the Fight Against Terrorism (adopted on 22 March 2005). The Republic of Armenia Criminal Code defines “an act of terrorism” and provides sanctions tailored to specific types of terrorist acts. Criminal responsibility for a terrorist act encompasses not only the perpetrator of the offense but also accomplices.
Company Registrar	https://www.e-register.am/en/search Website for the Legal Entities Search Service of the Ministry of Justice of the Republic of Armenia.
Access to Public Information	https://www.gov.am/en/inquiry-sample/ According to Article 9 of the Law of the Republic of Armenia on the Freedom of Information, individuals seeking to request information must provide a signed and sealed written request to the following e-mail: info@mfa.am
Other	https://foi.am/en Public website of Armenia and information relating to the Freedom of Information Centre of Armenia.

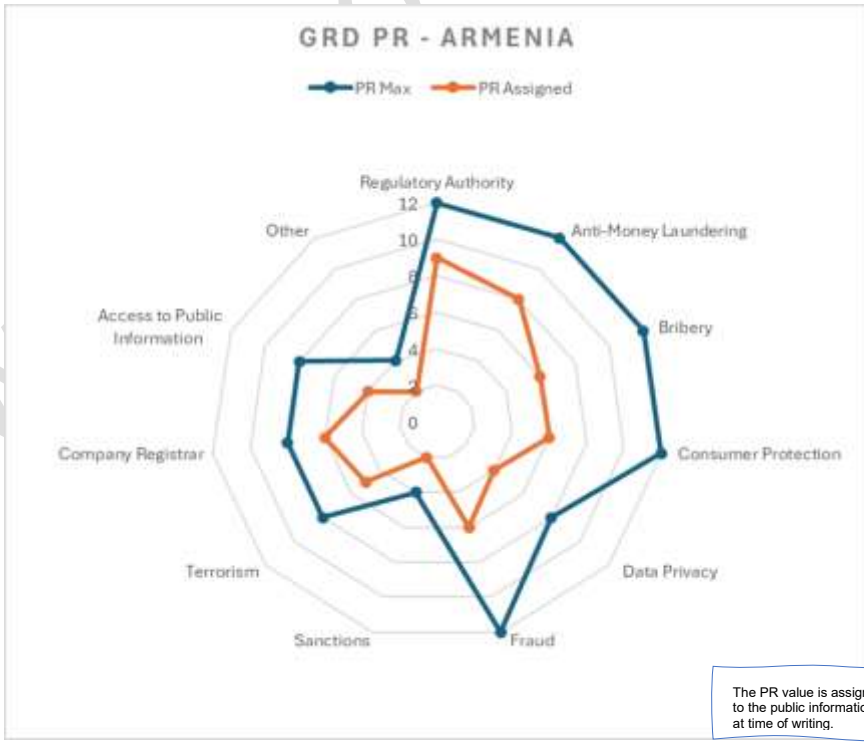
Posture Rating - Armenia

The PR value of **5.7** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	9	8	5	6	4	6	2	5	6	4	2

Armenia has a clear set of defined processes, regulations and laws to support domain obligations. As Armenia introduces more interconnected secure digital channels, we see the value rising, however, we did observe a weakness in the availability of public information and some advisory on the Data Privacy of its citizens.

N.B.: The figure does not reflect the execution of any processes, laws and regulations.



The PR value is assigned subject to the public information available at time of writing.

Australia

Commentary

Financial Regulatory Authority

https://www.rba.gov.au/ (i)
https://www.apra.gov.au/ (ii)
https://asic.gov.au/ and https://regulatoryportal.asic.gov.au/ (iii)

The Reserve Bank of Australia (RBA) is Australia's central bank and derives its functions and powers from the *Reserve Bank Act 1959*. In terms of the Act, there are two Boards: **The Reserve Bank Board** and the **Payments System Board**.

The Reserve Bank Board's commitments are to ensure the following;

The **Payments System Board** will best contribute to the overall stability of the financial system by:

1. Controlling and possible risk in the financial system
2. Promoting efficiency of the payments system
3. Promoting competition in the market for payment services, consistent with the overall stability of the financial system

(i)

The Australian Prudential Regulation Authority (**APRA**) is an independent statutory authority that supervises institutions across banking, insurance and superannuation and is accountable to the Australian Parliament. The APRA regulates 1,790 financial institutions as of 2024.

(ii)

The Australian Securities & Investment Commission (**ASIC**) is Australia's integrated corporate, markets, financial services and consumer credit regulator. The ASIC Portal is a rich source ASIC's suite of digital services.

(iii)

The legal currency of Australia is the Australian **dollar**.

Commentary

AI Act / Policy

URL

https://storage.googleapis.com/converlens-au-industry/industry/p/prj2452c8e24d7a400c72429/public_assets/safe-and-responsible-ai-in-australia-governments-interim-response.pdf (i)

https://www.industry.gov.au/science-technology-and-innovation/technology/artificial-intelligence (ii)

https://www.buyict.gov.au/sys_attachment.do?sys_id=ed35e2ca935caa10438b39cdfaba1039 (iii)

The Australian Government published its interim AI response to consultation on 17 January 2024.

(i)

The Australian Department of Industry, Science and Resources is responsible for AI Policy in Australia and recently published its "Developing the AI Ethics Principles", a set of eight core principles for the introduction of AI into the economy.

(ii)

Figure 4 The Australia AI Ethics Principles

Artificial Intelligence **(AI) model clauses** provide terms for purchasing AI systems, these clauses aim to help mitigate risks and promote transparency and accountability in AI deployment throughout the Australian Government.

(iii)

Anti-Money Laundering

URL

https://www.austrac.gov.au/about-us/what-we-do (i)

https://www.austrac.gov.au/business/new-to-austrac/enrol-or-register (ii)

https://www.austrac.gov.au/partners/government-partners (ii)

https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r7243 (iii)

The Australian Governments **AUSTRAC** is responsible for preventing, detecting and responding to criminal abuse of the financial system to protect the community from serious and organised crime.

(i/ii)

Site to enrol and create an online account with AUSTRAC, complete the AUSTRAC Business Profile Form (**ABPF**) online. N.B. Foreign Companies must supply registration details if registered outside of Australia.

AUSTRAC works closely with a range of Australian government partners to protect the community from serious crime and terrorism. The list of partners can be found via the Government website.

(iii)

On 29 November 2024, Parliament passed the Anti-Money Laundering and Counter-Terrorism Financing (**AML/CTF**) **Amendment Bill**, amending the **AML/CTF Act 2006**. The new laws reform Australia's AML/CTF regime to ensure that they can more effectively deter, detect and disrupt crimes like money laundering, terrorism financing and proliferation financing.

(iv)

Commentary

Bribery

https://www.ag.gov.au/crime/foreign-bribery (i)
https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=s1246 (ii)

The Attorney General's website regarding foreign bribery offences and penalties. N.B. While reporting suspected criminal activity to the AFP is not an offence, making a report that is vindictive or malicious, knowing the allegations are unfounded, may be an offence.

(i)

Crimes Legislation Amendment (Combatting Corporate Crime) Bill 2019.

(ii)

Consumer Protection

https://consumer.gov.au/ (i)
https://www.legislation.gov.au/C2004A00109/latest/text (ii)
https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r4180 (iii)

The Australian Consumer Law (**ACL**) is a single, national law, which applies in the same way nationally and in each state and territory. It is the principal consumer protection law in Australia.

(i)

The ACL includes:

1. A national unfair contract terms law covering standard form consumer and small business contracts;
2. A national law guaranteeing consumer rights when buying goods and services;
3. A national product safety law and enforcement system;
4. A national law for unsolicited consumer agreements covering door-to-door sales and telephone sales;
5. Simple national rules for lay-by agreements; and
6. Penalties, enforcement powers and consumer redress options.

The Australian Consumer Law (ACL) - set out in Schedule 2 of the **Competition and Consumer Act 2010**.

(ii)

The Australian credit card laws are regulated by the **National Consumer Credit Protection Act (2009)**.

(iii)

Cloud Policy

https://www.infrastructure.gov.au/sites/default/files/2014-112101-CLOUD-Consumer-factsheet.pdf (i)
https://www.ospi.es/export/sites/ospi/documents/documentos/Australian-Government-cloud-computing-policy.pdf (ii)

Cloud Computing and Privacy Consumer Fact sheet.

(i)

Australian Government Cloud Computing Policy.

(ii)

Commentary

Data / Privacy

https://www.legislation.gov.au/Series/C2004A03712 (i)
https://www.oaic.gov.au/privacy/australian-privacy-principles (ii)

The Privacy Act 1988 (**Privacy Act**) is the principal piece of Australian legislation protecting the handling of personal information about individuals.

The thirteen Australian Privacy Principles (or **APPs**) are the cornerstone of the privacy protection framework in the Privacy Act 1988. They apply to any organization or agency the Privacy Act covers.

(ii)

Fraud

https://www.cdpp.gov.au/crimes-we-prosecute/fraud/general-fraud

In Australia, every state and territory have an offence involving dishonestly gaining property or a financial advantage, also known as fraud, deception, or dishonestly acquiring a financial advantage. These offences are serious and can attract lengthy terms of imprisonment.

Commentary

Sanctions

https://www.dfat.gov.au/international-relations/security/sanctions

Australia implements two types of sanctions:

1. United Nations Security Council (**UNSC**) sanctions, which Australia must impose as a member of the UN.
2. Australian autonomous sanctions, which are imposed as a matter of Australian foreign policy. The Australian Sanctions Office (**ASO**) is the Australian Government's sanctions regulator and sits within **DFAT's** Regulatory Legal Division in the Security, Legal and Consular Group.

Australian sanction laws apply broadly, including to activities:

1. Within Australia;
2. By Australian citizens and Australian-registered bodies corporate overseas; and
3. On board Australian-flagged vessels and aircraft.

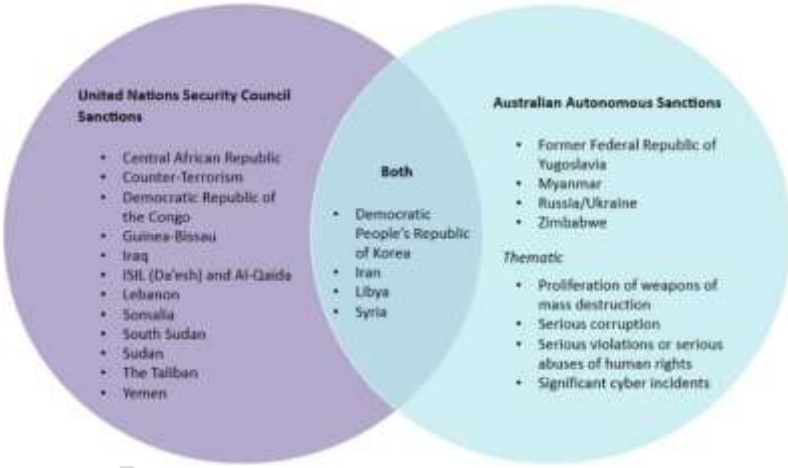


*Figure 5 Australian Sanctions regimes and laws (**Data Source** :DFAT website Jan 2025)*

Terrorism

https://www.austrac.gov.au/about-us/what-we-do

The Australian Government's AUSTRAC performs a dual role as Australia's anti-money laundering (**AML**) and counter-terrorism financing (**CTF**) regulator and financial intelligence unit.

Commentary

Company Registrar

https://asic.gov.au/ (i)

https://connectonline.asic.gov.au/RegistrySearch/faces/landing/SearchRegisters.jspx?_adf.ctrl-state=y13op2s5m_4 (ii)

https://connectonline.asic.gov.au/RegistrySearch/faces/landing/ProfessionalRegisters.jspx?_adf.ctrl-state=8penjeiiy_12 (ii)

To register a company in Australia officially, one can visit the **Australian Securities & Investments Commission (ASIC)**.

(i)

ASIC provide an online search system to look up all Australian registered companies.

(ii)

It should be noted that anyone who sells financial or investment product or gives financial advice in Australia must have an Australian financial services (**AFS**) licence which can be validated at the URL shown.

(iii)

Access to Public Information

https://www.oaic.gov.au/freedom-of-information

The **Australian Freedom of Information Act 1982** (**FOI Act**) gives citizens the right to request access to government-held information.

Other

https://www.pm.gov.au/ (i)

https://my.gov.au/ (ii)

https://www.ags.gov.au/ (iii)

The Australian government has multiple websites with the suffix.gov.au.

The official website of the Prime Minister.

(i)

The official portal to access government services.

(ii)

The Australian Government's central legal service(**AGS**)

(iii)

Posture Rating Australia

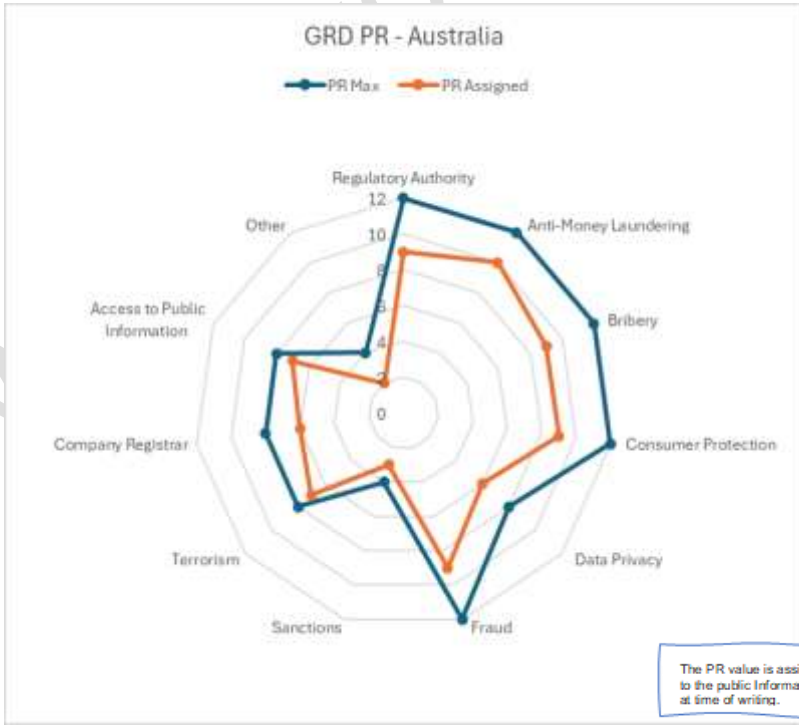
The PR value of **7.7** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	9	10	9	9	6	9	3	7	6	7	2

Australia has a set of mature, well-defined processes, regulations and laws to support its domain obligations.

We did not observe any major restrictions on digital channels and a good level of recent content publication on its websites.

N.B.: The figure does not reflect the execution of ay processes, laws and regulations.



Republic of Austria

Commentary

Financial Regulatory Authority

https://www.oenb.at/en/ (i)
https://www.oenb.at/dam/jcr:145ade8d-3de9-443a-b03a-081d4eb40a86/federal_act_1984_june_2018.pdf (ii)
https://www.fma.gv.at/en/ (iii)

The central bank of the Republic of Austria is the Oesterreichische National bank (**OeNB**).

(i)

The OeNB is a stock corporation under the Federal Act on the Oesterreichische National bank 1984 (Nationalbank Act). Its nominal capital of eur 12 million is held in its entirety by the central government. The shareholder rights of the federal government are exercised by the Federal Minister of Finance.

(ii)

With Austria entering the third stage of Economic and Monetary Union (EMU) on January 1, 1999, the OeNB became an integral part of the European System of Central Banks (ESCB). However, the OeNB remains a fully independent national central bank.

The Financial Market Authority (**FMA**) is Austria's financial supervisory authority and supervises, inter alia, credit institutions, securities markets and brokers, fund managers, pension funds, payment services providers, investment firms and insurance companies.

(iii)

As a member of the European Community, Austria has adopted the **euro** as the common currency.

AI Act / Policy

https://www.digitalaustria.gv.at/eng/strategy/strategy-AI-AIM-AT-2030.html

In 2021, the Government issued its federal strategy on AI – the Artificial Intelligence Mission Austria 2030 (**AIM AT 2030**).

AIM AT 2030 sets the guidelines in which the use of AI in Austria can and should develop. At the same time, AIM AT 2030 focuses on agile, interdisciplinary and participatory implementation and further development.

Anti-Money Laundering

https://www.fatf-gafi.org/en/countries/detail/Austria.html (i)
https://www.parlament.gv.at/gegenstand/XXV/I/1346 (ii)

Austria reported back to the FATF in 2017 and 2018 on the actions it had taken to strengthen its AML/CFT framework. Austria reports it is compliant with eighteen recommendations, largely compliant with another 18 Recommendations, but remains partially compliant with four Recommendations.

(i)

The "Fourth Anti-Money Laundering Directive" (Directive 2015/849/EU) considering the FATF-recommendations has been implemented in the Austrian Act Amending Professional Rules and Regulations 2016 (Berufsrechts-Änderungsgesetz 2016 – BRÄG 2016, BGBl [Federal Law Gazette] I 10/2017) by *specifying the legal professionals' obligations in combatting money laundering and terrorist financing for lawyers and civil law notaries*. The relevant stipulations particularly can be found in Section 8a to 8f Lawyer's Act and Section 36a to 36f Notarial Code.

(ii)

Commentary

Bribery

https://www.bmeia.gv.at/en/european-foreign-policy/global-issues/anti-corruption (i)
https://bak.gv.at/en/start.aspx (ii)
https://bak.gv.at/en/101/files/BAK-G_Fassung_vom_29022024__uebersetztBAK418_eng-GB_bf.pdf (iii)

Austria ratified the OECD Anti-Bribery Convention on 20 May 1999. The convention establishes legally binding standards to criminalise bribery of foreign public officials in international business transactions and provides for a host of related measures that make this effective.

Further information can be found on the Anti-Corruption page of the Federal Ministry of Austria's website – European and International Affairs.

(i)

The Federal Bureau of Anti-Corruption (**BAK**) is the institution of the Austrian Federal Ministry of the Interior and was established outside the Directorate-General for Public Security with nationwide jurisdiction for the:

1. Prevention of and the fight against corruption
2. Close cooperation with the Public Prosecutor's Office for White-Collar Crime and Corruption (**WKStA**)
3. Security police and criminal police cooperation with foreign and international anti-corruption institutions

(ii)

The "Entire legal provision for the Act on the Federal Bureau of Anti-Corruption (Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung or BAK), version of 29 February 2024" refers to Bribery (**307 Penal Code**) under the BAK Remit.

(iii)

Consumer Protection

https://www.sozialministerium.at/en/Topics/Consumer-Protection.html (i)
https://www.oesterreich.gv.at/en/themen/gesetze_und_recht/verbraucherschutz.html (ii)

Consumer protection in Austria falls under the control of the Social Affairs, Health Care and Consumer Protection division of the Federal Ministry **(i)** and is encapsulated by several laws and regulations, including:

1. The Austrian General Civil Code (**ABGB**): Contains general regulations on contracts, warranties and more
2. The Consumer Protection Act (**KSchG**): Contains special regulations on contracts between consumers and companies
3. The Act against Unfair Competition (**UWG**): Protects consumers from unfair business practices and misleading behaviour

Public information and services of the Austrian administration.

(ii)

Cloud Policy

https://www.fma.gv.at/en/eu/eiopa-guidelines/

The use of Cloud Services is permissible in Austria; however, Cloud Services are subject to various Austrian Consumer Protection , EBA and EU Laws e.g. the Guidelines issued under Article 16 of Regulation (EU) **No 1094/2010**.

Commentary

Data / Privacy

https://www.data-protection-authority.gv.at/ (i)
https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1999_1_165/ERV_1999_1_165.html (ii)

The Austrian Data Protection Authority is the national supervisory authority for data protection in the Republic of Austria.

(i)

The Austrian data protection act (Datenschutzgesetz, short DSG) supplements the EU GDPR.

(ii)

Fraud

https://www.bmf.gv.at/en/the-ministry/internal-organisation/Anti-Fraud-Office-.html

Under Austrian criminal law, Fraud is covered in sections **146** to **148** of the Penal Code (Strafgesetzbuch, StGB) and regulated by the Anti-Fraud Office (**ABB**).

Fraud is classed as a **property crime** when offenders intentionally deceive victims by making false representations or concealing facts with the intention of unlawfully enriching themselves and thereby causing financial loss to a third party.

Sanctions

https://www.oenb.at/en/About-Us/legal-framework/reporting-obligation-for-sanctioned-persons.html

URL for the Reporting obligation for sanctioned persons i.e. Reports under Article 9 Council Regulation (EU) **269/2014** as amended.

The reporting template is available at the OeNB website (available in German) which should completed and sent by email to sanktionen@oenb.at

Terrorism

https://www.bmeia.gv.at/en/european-foreign-policy/global-issues/international-counter-terrorism

Austria remains fully committed to the fight against terrorism, extremism and radicalisation and all international efforts to combat terrorist activities.

The important **Criminal Law Amendment Act 2018** broadened the group of persons that are afforded legal support for criminal proceedings upon request by now explicitly including victims of terrorist offences according to section **278c** of the **Austrian Criminal Code** [Strafgesetzbuch (StGB)] in section **66** para. 2 of the **Austrian Code of Criminal Procedure** (**CCP**).

The Criminal Law Amendment Act 2018 also led to the:

1. Extension of the domestic jurisdiction concerning terrorism,
2. Extension of terrorist offences,
3. Extension of criminal offences suitable for financing terrorism as well as,
4. Introduction of the new criminal offence, travelling for terrorist purposes in section **278g** of the Austrian Criminal Code.

Commentary

Company Registrar

https://www.fma.gv.at/en/search-company-database/ (i)

https://justizonline.gv.at/jop/web/firmenbuchabfrage (ii)

A Company Database Search service from the Austrian Financial Market Authority. (i)

JustizOnline is the digital information service of the Austrian judiciary and provides a simple tool to lookup companies registered in the Austrian Commercial Register. (ii)

Access to Public Information

https://www.parlament.gv.at/gegenstand/XXVII/I/2238 (ii)

From September 2025 the Freedom of Information Act will come into force where official secrecy will be abolished and access to government information will be facilitated. The Link provided is to the Federal Act amending the Federal Constitutional Act and enacting a Freedom of Information Act.

Other

https://www.oesterreich.gv.at/en/public.html (i)

https://www.fatf-gafi.org/en/countries/detail/Austria.html#:~:text=As%20a%20result%2C%20the%20FATF,partially%20compliant%20with%204%20Recommendations. (ii)

Official website for Digital Government Services. (i)

Austria was examined by the FATF in 2015/2016. The assessment report was published in September 2016 and is available on the FATF website. (ii)

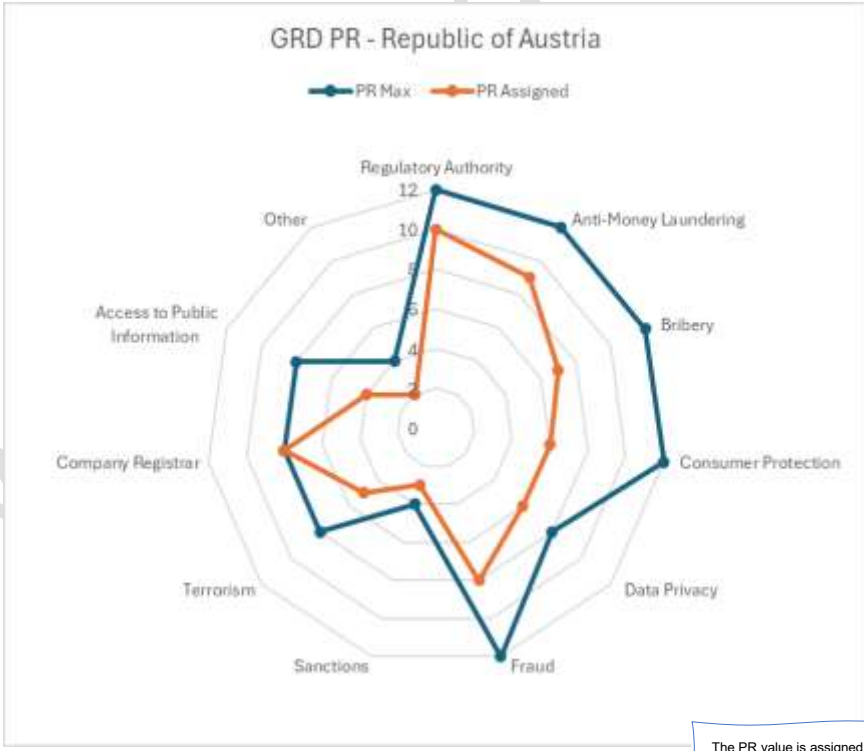
Posture Rating Austria

The PR value of **6.8** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	**12**	**12**	**12**	**12**	**8**	**12**	**4**	**8**	**8**	**8**	**4**
PR Assigned	10	9	7	6	6	8	3	5	8	4	2

Austria has adopted many of the EU processes, regulations and laws to support its domain obligations. However, some observed weaknesses in some of the domains e.g. the Freedom of Information Act will not be enforced until Sept 2025.

N.B.: **The figure does not reflect the execution of any laws and regulations**.



The PR value is assigned subject to the public information available at time of writing.

Kingdom of Bahrain

Commentary

Financial Regulatory Authority

https://www.cbb.gov.bh/ (i)

https://cbben.thomsonreuters.com/cbb-rulebook (ii)

The Central Bank of Bahrain ('CBB') is a public corporate entity established by the Central Bank of Bahrain and Financial Institutions Law 2006. It was created on 6th September 2006.

The CBB is responsible for maintaining monetary and financial stability in the Kingdom of Bahrain. It is also the single integrated regulator of Bahrain's financial industry.

(i)

Bahrain's banking system consists of both conventional and Islamic banks and is the largest component of the financial system.

The CBB Rulebook represents the main source of Regulatory Controls for the Kingdom of Bahrain with changes to the Rulebook generally made on a quarterly cycle *(the only exception being when changes are urgently required*).

(ii)

The Bahraini **dinar** is the official currency of Bahrain.

AI Act / Policy

https://www.bahrain.bh/wps/portal/en/!ut/p/z0/fcy7DsIwDEDRX8nSOeFVWBFCPKYKMUAW5KYmmKZ2Wwzi88kXMB7p6IpvL9YzfCiCkjCk7Ksvb5PDwu1XG-f25XnqyvVuOauq7cSd5vZo_f8gH-g5DH5tfRBW_Kq91NzfkAsHtbzV6ANNSxwb6QqHHY4xwyiGB0uSSPgq3IgJFBuj0lPIhlHpToEgGcrTlCgiBzTAjRmlFs2V7Vt__QFQy9m1/ (i)

https://www3.weforum.org/docs/WEF_AI_Procurement_in_a_Box_Challenges_and_Opportunities_during_implementation_2020.pdf (ii)

When selecting the URL link (i), one is presented with a summary of the Activity in the Kingdom with regards to Artificial Intelligence which currently centres on the following areas;

1. AI for **Agriculture** – Using AI to count Palm Trees
2. AI **Certification** – The Bahrain Academy program receives professional certification, as well as a certificate of attendance by Bahrain Polytechnic upon program completion
3. AI **Research** - The government of Bahrain approved the establishment of a national research in the field of AI
4. AI in **Courtrooms** - Bahrain is actively exploring ways to improve the efficiency in courtrooms and throughout the judiciary system
5. The Chatbot Project is currently underway by the Information and **eGovernment** Authority
6. AI in **Procurement** (*See ii*)

Commentary

Anti-Money Laundering

https://www.moic.gov.bh/sites/default/files/2021-10/1.%20Decree%20Law%20No.%204%20of%202001%2C%20with%20Respect%20to%20the%20Prevention%20and%20Prohibition%20of%20the%20Laundering%20of%20Money..pdf (i)

https://www.moic.gov.bh/en/node/2867 (ii)

Decree Law No. 4 of 2001 prohibits and prevents money laundering. Order no. 173 of 2017 sets out the obligations of businesses to combat money laundering and terrorism financing.

(i)

The URL for the **Ministry of Industry and Commerce** - AML Department providing information for the Bahrain national domestic sanctions list (in Arabic).

(ii)

Bahrain is member of the Financial Action Task Force ('FATF') via its full membership of the Gulf Cooperation Council in the FATF.

Bribery

https://www.cbb.gov.bh/wp-content/uploads/2018/12/Decree-No.-25-of-2013.pdf

There is currently **no specific law governing anti-bribery** and corruption. However, there are provisions encapsulated within other laws that provide for bribery related offenses which are punishable under Bahraini law.

The bribery offences describe a bribe as a **gift or privilege of any kind** whatsoever or a promise to be given the same, either directly or indirectly, to induce or reward the improper performance of a relevant function or activity.

Consumer Protection

https://bahrain.bh/wps/portal/en/BNP/YourGuideForLivingInBahrain/ConsumerProtectionAndRetails (i)

https://services.bahrain.bh/wps/portal/tawasul/en (ii)

The official eService Consumer Protection and Retails site for the Government of Bahrain.

(i)

The **Tawasul** platform connects citizens with more than 56 governmental entities and provides the following services:

1. **Submit enquiries and complaints:** Get a response to enquiries or feedback on any service-related issues directly from the relevant government entity according to a pre-defined performance indicator and timeframe.
2. **Share Suggestions**: Post suggestions and opinions.
   NB. this is *not anonymous and* name and passport details are requested on entry.
3. **Expression of gratitude and appreciation**: Recognizing outstanding service from specific employees or government to encourages continuous improvement of government customer experience.

(ii)

Commentary

Cloud Policy

https://www.bahrain.bh/wps/wcm/connect/d8f92e07-886c-4a1e-94f8-3abcb9b7cfbf/CloudFirstPolicy.pdf?MOD=AJPERES&CVID=og9l.SG (i)

https://cic.polytechnic.bh/ (ii)

The Kingdom of Bahrain published the **Cloud First Policy** in 2017 with the aim:

1. Reducing the cost of government ICT by eliminating duplication of solutions and fragmentation in the technology environment and leveraging the efficiencies of on-demand provisioning of ICT services;
2. Increasing security by using accredited platforms;
3. Increasing productivity and agility and thus improving citizen services.

(i)

The Bahrain Polytechnic Cloud Innovation Centres (CIC) Program enables nonprofits, educational institutions and government agencies to team up with fellow public sector organizations. Together, they can tackle challenges and experiment with innovative solutions using Amazon's technology and its Amazon Web Services (**AWS**) platform.

(ii)

Data / Privacy

https://www.bahrain.bh/wps/wcm/connect/ab8b334e-8c6f-4ff9-90b6-94135da559ca/Law+No.+%2830%29+of+2018+DPL.pdf?MOD=AJPERES&CVID=oFapPNI

Law No.30 of 2018 covers the provisions for automated data processing, in whole or in part, the general legality framework, the provisions for the transfer of personal data outside the Kingdom and the establishment and organization of the competent authority.

Fraud

https://bahrain.bh/wps/portal/en/BNP/HomeNationalPortal/ContentDetailsPage/!ut/p/z1/lVNLc4IwEP4r9OCRyfIK4Yh1FDtjtSoqXBweEVIhIEbtz2_oTa2vPWV3vt1vH19QiFYo5NGRZZFgFY8K6QchXmtDCzzyDjDpmTp8LZwp7o40GA0MtDwHaHMfJGDoTsf9ngamhsJn8uGGufBc_h1AeL_8Rb4zdzBgXXdNfTYwYPyQf4FCFNYJS1FALYKJDRtVIwlVTZJEKnFwquJ4E6eOnZgYWy064aIWOQpiXq8p70AUVwehiJwqW8aztCpliAumJlXTHOr2EFeBtsxeoI_z7rzPSQ_w2CO2bneN8cRoz8e-d7vQlawVF_RHoNUd2jjKm4hxphQ0Y_viTwT7DjRUPmmqiKpmifSTnBWp0rAsF_vLHq439GIPD0dftsOf3cz3-4DJoG-amExty74E_CPKR7IlpCzsm1MNpe6OjJ6Qz6umlN9k9qIKPEAzylFd-tJKYnCrOJZLdTslp_kme_sFVkYbRA!!/

Law 62 of 2014 (the new Commercial Anti-Fraud Law), was enacted in October 2014 and established additional grounds to trademark owners to file a complaint before the Bahraini authorities to pursue and impose sanctions against traders and entities that supply counterfeit products, including foodstuffs, basic and luxury products, medical products, cosmetics and other commodities.

The Law also criminalizes the attempt to *commit fraud by giving false information* about the type, origin or source. Interestingly, the sanctions of the Law are substantial and in addition to other types of fraud can be used to pursue infringers of intellectual property rights. However, this does not prejudice the use of any more severe punishment stipulated in other laws, such as trademarks or penal codes in Bahrain. This reflects the legislator's intent to impose high penalties against those that commit fraud, including counterfeiting traders and for the penalties to comprise both imprisonment and fines.

Sanctions

The Government of Bahrain may from time-to-time designate certain individuals and organizations as being linked to the financing of terrorism, for instance when so designated by the United Nations. These names are circulated to the financial sector by the Central Bank of Bahrain.

Commentary

Terrorism

Bahrain has identified some divisions of non-profit organizations for potential abuse and applies restrictive obligations on all non-profit organizations operating in Bahrain.

AML/CFT Legislative Decree no. (4) of 2001 Concerning the Prohibition of and Combating Money Laundering was amended by **Law No. 54 of 2006**, which adds a specific prohibition on the financing of terrorist organizations or their members.

Refer to AML URL above.

Company Registrar

URL https://www.bahrainchamber.bh/en/businesses-search

The Bahrain Chamber of Commerce and Industry (**BCCI**) provides an online search capability that allows one to search for various legal entities in the region, which can be one of the following;

1. Audit Firms
2. Bahrain Shareholding Companies (Public)
3. Branch of a Foreign Company
4. Closed joint Stock Co (Foreign Capital Co)

Access to Public Information

URL https://www.bahrain.bh/wps/wcm/connect/1d60cf1c-d6e2-4835-8631-7f35505980cf/%D9%85%D8%B1%D8%B3%D9%88%D9%85+%D8%A8%D9%82%D8%A7%D9%86%D9%88%D9%86+%D8%B1%D9%82%D9%85+%2847%29+%D9%84%D8%B3%D9%86%D8%A9+2002+%D8%A8%D8%B4%D8%A3%D9%86+%D8%AA%D9%86%D8%B8%D9%8A%D9%85+%D8%A7%D9%84%D8%B5%D8%AD%D8%A7%D9%81%D8%A9+%D9%88%D8%A7%D9%84%D8%B7%D8%A8%D8%A7%D8%B9%D8%A9+%D9%88%D8%A7%D9%84%D9%86%D8%B4%D8%B1.pdf?MOD=AJPERES&CVID=o8Q1lTg Arabic

The Kingdom promotes the fact that it has made great strides in ensuring freedom of opinion and expression and freedom of the press in accordance with its constitutional and legal frameworks. Decree No. (47) of 2002 regulates the press, printing and publishing.

Other

URL https://services.bahrain.bh/wps/portal/ar/BSP/HomeeServicesPortal/ (i)
https://www.bahrain.bh/wps/portal/en/BNP/GSX-UI-AllEntities/ (ii)
https://www.cbb.gov.bh/wp-content/uploads/2021/05/Consultation_Vol-1_FC_E-KYC.pdf (iii)

National Portal of the Kingdom.

(i)

Government Directory providing a comprehensive guide to ministries, authorities and government institutions in the Kingdom of Bahrain.

(ii)

Any financial institution licensed by the Central Bank of Bahrain is required to perform *Know Your Customer* (KYC) as per the **Central Bank of Bahrain Rulebook.**

(iii)

Posture Rating Bahrain

The PR value of **6.6** is derived using the following assigned values:

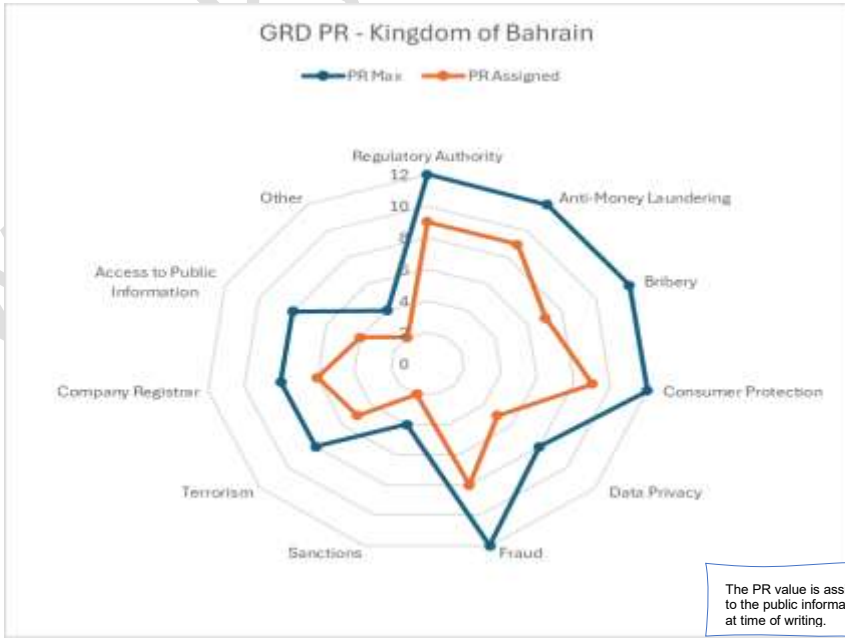
	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	10	9	7	9	5	8	2	5	6	4	2

The Kingdom of Bahrain has set to define multiple processes, regulations and laws to support its domain obligations.

We found the CBB Rulebook, which is utilized across various domains, to be a well-articulated document regarding outlining regulatory controls. As a result, it positively impacted the overall PR rating attributed to the Regulatory Authority.

However, we observed weaknesses in some domains, which was not helped by the lack of non-Arabic documents available to us.

NB: **The figure does not reflect the execution of any of these laws or regulations.**



The PR value is assigned subject to the public information available at time of writing.

Bangladesh

Commentary

Financial Regulatory Authority

https://www.bb.org.bd/en/index.php (i)

https://www.bb.org.bd/monetaryactivi-ty/mps/mps_h1fy25.pdf (ii)

Bangladesh Bank is the central bank of Bangladesh and is a member of the Asian Clearing Union. It is fully owned by the Government of Bangladesh.

(i)

Bangladesh Bank's 2024 monetary policy was largely influenced by trends and changes to in key indicators because of three key policy pillars:

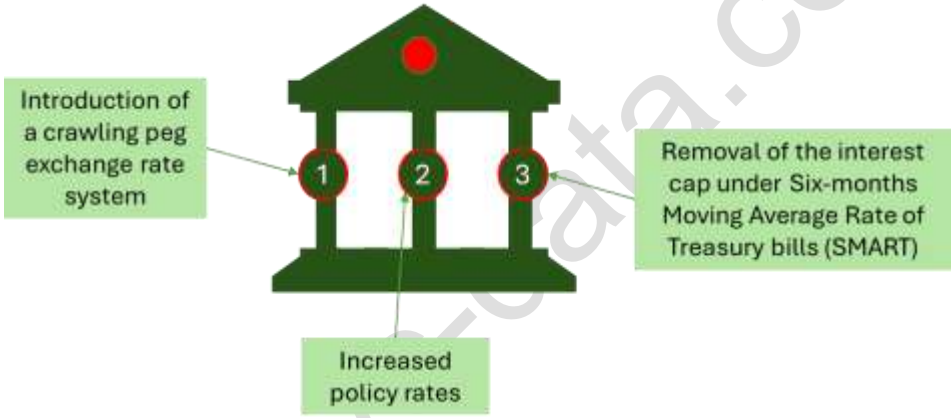


Figure 6 BB's Three Key Policy Pillars

The main functions and aims of Bangladesh Bank are as follows:

1. To formulate monetary and credit policies
2. Stabilise currency and regulate payment systems
3. Manage foreign exchange rate reserves and regulate the foreign exchange market
4. Regulate and supervise banks and other financial institutions
5. Provide the Government of Bangladesh guidance with regards to shaping fiscal, monetary and economic policies

(ii)

The Bangladeshi **taka** is the currency of the People's Republic of Bangladesh.

Commentary

AI Act / Policy

https://ictd.portal.gov.bd/sites/default/files/files/ictd.portal.gov.bd/policies/e57f1366_a62c_4d1a_8369_a9d3bc156cd5/National%20Strategy%20for%20Artificial%20Intelligence%20-%20Bangladesh%20.pdf

In 2020, the Information and Communication Technology Division of the People's Republic of Bangladesh issued the **National Strategy for Artificial intelligence Bangladesh.**

The main aims of the strategy were to provide a comprehensive framework for Bangladesh in becoming a 'technologically advanced nation' within the next 10 years and embracing the full potential of ICT as a tool for sustainable development.

The strategy is comprised of the following six key strategic goals:

1. Research and development
2. Skilling and reskilling of AI in the workforce
3. Data and digital infrastructure
4. Ethical, data privacy and security considerations in relation to regulating AI
5. Funding and accelerating AI start-ups
6. Industrialisation of AI technologies

Anti-Money Laundering

https://www.bb.org.bd/aboutus/regulationguideline/aml/aml-cft-guidelines.pdf (i)
https://www.bb.org.bd/aboutus/regulationguideline/aml-cft_dnfbp_oct2013.pdf (ii)
http://bdlaws.minlaw.gov.bd/act-details-1088.html?lang=en (iii)

Bangladesh Bank issued Guidelines on Prevention of Money Laundering and Combatting Financing of Terrorism (AML/CFT) for Capital Market Intermediaries. The purpose of these guidelines is to ensure appropriate identification information can be obtained regarding Capital Market Intermediaries (CMIs), aiding the detection of suspicious transactions and creating an 'effective audit trail'.

(i)

The Government of Bangladesh also issued **Guidelines on Prevention of AML/CFT for Designated Non-financial Business and Professions (DNFBP), 2013.** This provides a framework for DNFBP's regarding implementing preventative measures against money laundering/terrorist financing related issues.

(ii)

Bangladesh's policies regarding anti-money laundering are also largely influenced the FATF (whom they are an associate member of). For example, considering the FATF's 40 recommendations, the Bangladesh Government issued the **Money Laundering Prevention Act, 2012,** aiming to align them more closely with international standards and initiatives.

(iii)

Commentary

Bribery

http://bdlaws.minlaw.gov.bd/act-217.html (i)
https://acc.org.bd/site/view/law/Act-&-Rule 2019 amended document (ii)

One of the first significant pieces of legislation pertaining to anti-bribery in Bangladesh is the **Prevention of Corruption Act 1947.** This establishes bribery as a criminal offence under Bangladesh law.

(i)

The Government of Bangladesh also issued the **Anti-Corruption Commission Act, 2004** (amended most recently in 2019). This was introduced as a further attempt to combat bribery and corruption in Bangladesh by establishing an independent **Anti-Corruption Commission**, responsible for conducting inquiries and investigations of corruption and other related offences.

The full documents are available to download from the official Anti-Corruption Commission website.

(ii)

Consumer Protection

http://bdlaws.minlaw.gov.bd/act-1014.html?lang=en
also available to download in English.

In 2009, the Ministry of Law, Justice and Parliamentary Affairs issued **The Consumer's Right Protection Act.** The act was implemented to prevent anti-consumer right practices occurring within Bangladesh and clearly stipulate the rights of consumers.

The main elements of the 2009 Act are as follows:

1. Establishing the National Consumer's Right Protection Council, responsible for devising and enforcing consumer protection regulations
2. Stipulating the powers and responsibilities of the Directorate of the National Consumer's Right Protection Council
3. Providing a comprehensive list of punishments for those in breach of consumer protection law in Bangladesh

The Central Bank of Bangladesh maintains a Customers' Interest Protection Center (CIPC) where complaints can be made via an online form[2] or via email to bb.cipc@bb.org.bd

Cloud Policy

https://ndc.bcc.gov.bd/wp-content/uploads/2023/06/NDC-Cloud-computing-policy-2023V1.0-Draft.pdf (i)

The Government department responsible for overseeing all matters in relation to cloud services in Bangladesh is the **National Data Centre (NDC).** They are implementing cloud services for Government and non-government organizations, ensuring compliance with global standards and accepted procedures.

The Government of Bangladesh does not currently have any direct regulation/strategy with regards to cloud computing. However, in 2023 the NDC drafted a **Cloud Computing Policy,** which upon release, aims to promote the development of cloud computing infrastructure in Bangladesh and ensure compliance with relevant domestic laws and regulations.

[2] Link not documented as the online submission URL was not valid at time of writing – recommend visiting the Bank's website.

Commentary

Data / Privacy

https://www.cirt.gov.bd/wp-content/uploads/2020/02/Digital-Security-Act-2020.pdf

There are currently no specific data protection laws or regulations that have been publicly issued in Bangladesh. There are various laws that coincide with data protection/privacy. For example, the **Digital Security Act of 2020** outlines what constitutes unlawful data collection and storage in Bangladesh.

Fraud

http://bdlaws.minlaw.gov.bd/act-26/section-179.html (i)

https://www.bb.org.bd/aboutus/regulationguideline/aml/aml-cft-guidelines.pdf (ii)

The Contract Act, 1872 defines fraud and outlines the various instances whereby an individual would be convicted of fraud. (i)

Bangladesh's strategy for tackling fraud is enshrined within the **AML/CFT Guidelines** issued by the Bangladesh Bank. (ii)

Sanctions

https://www.mofa.gov.bh/en/combating-terrorism-and-extremism

Link to the Bangladesh Bank's Domestic sanctions list – this can also be viewed at the www.kyc-data.com portal.

Terrorism

https://www.bb.org.bd/aboutus/regulationguideline/aml-cft_dnfbp_oct2013.pdf

The Department of Home Affairs for the Government of Bangladesh issued the **Anti-Terrorism Act** of 2009 (most recently amended in 2012).

Following on from the act of 2009, the government authority also issued a comprehensive document outlining the **Anti-Terrorism Rules (2013).** Some of the key elements of this publication are as follows:

1. Granting the **Bangladesh Financial Intelligence Unit (BFIU)** powers to freeze and suspend suspicious transactions
2. Outlining the duties of the **Proscription and Enlistment Committee**
3. Providing a framework for implementing the provisions of the **UN Council Resolutions**
4. Investigation and trial procedures

Commentary

Company Registrar

https://roc.portal.gov.bd/
https://dbid.gov.bd/
https://www.sec.gov.bd/

The Government Department - Office of the **Registrar of Joint Stock Companies** and Firms.

(i)

DBID is a government platform that aims to bring together businesses in Bangladesh. It helps organizations, domestic and foreign business entities, micro-merchants, financial institutions and the rest to register and get a unique business identification number for their respective businesses digitally.

(ii)

The Bangladesh Securities and Exchange Commission (**BSEC**) is the regulator of the country's capital market under the provision of Bangladesh Securities and Exchange Commission Act 1993. The purpose of the Commission is to protect the interest of investors in securities, develop the securities market and make rules for matters ancillary or connected.

(iii)

Access to Public Information

https://sid.gov.bd/ (i)
http://data.gov.bd/dataset (ii)
http://data.gov.bd/request-dataset (iii)

In 2016, the Government of Bangladesh issued its **Open Government Data Strategy.** This main purpose of this was to encourage innovative solutions in the public sector through broadening the scope for research and development, creating new employment and investment opportunities and making the government more transparent and accountable.

The full document is available to download from the official Bangladesh National Portal- Statistics and Information Division under the OGD section.

(i)

Public data can be accessed via the official Bangladesh Open Data website.

(ii)

Information not already publicly available may be requested via the Open Data website.

(iii)

Bangladesh promotes *"Freedom of thought and conscience and of speech"* under – Article 39 of the Constitution makes provisions for ensuring free flow of information and citizen's right to information - See link (iii) in Other below.

Other

https://bangladesh.gov.bd/index.php (i)
https://mofa.gov.bd/ (ii)
http://bdlaws.minlaw.gov.bd/act-367.html (iii)

The official Government website.

(i)

Ministry of Foreign Affairs public website.

(ii)

The constitution of the people's republic of Bangladesh.

(iii)

Posture Rating Bangladesh

The PR value of **6.9** is derived using the following assigned values:

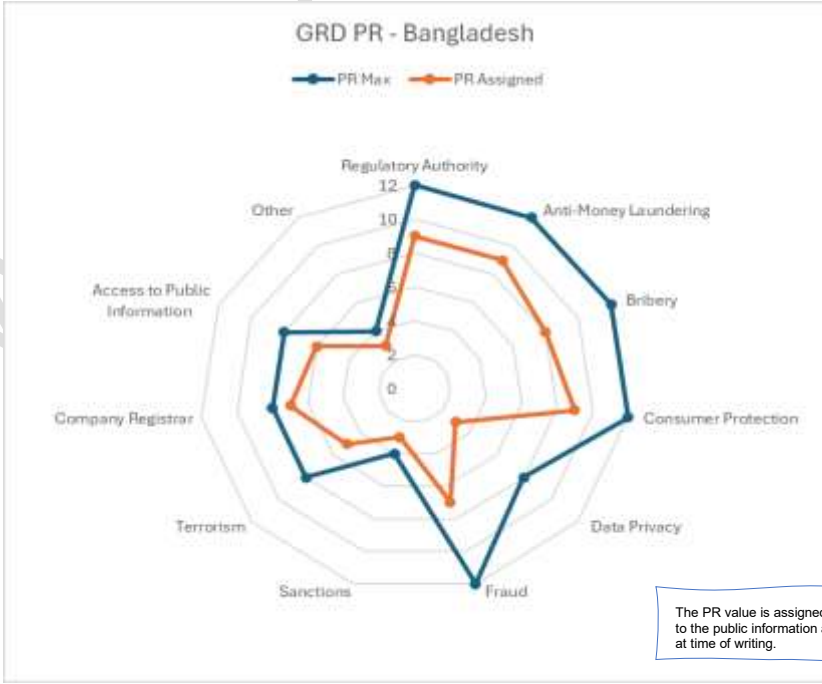
	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	9	9	8	9	3	7	3	5	7	6	3

Bangladesh has specified and continues to introduce new processes, regulations and laws to meet its domain obligations.

Whilst Data Privacy contributed a low score, we did observe in other areas the welcome introduction of counter measures e.g. the central bank's complaint hotline.

It should be noted that on some value adding services URLs did not pass our integrity end point check.

NB: **The figure does not reflect the execution of any of these laws or regulations**.



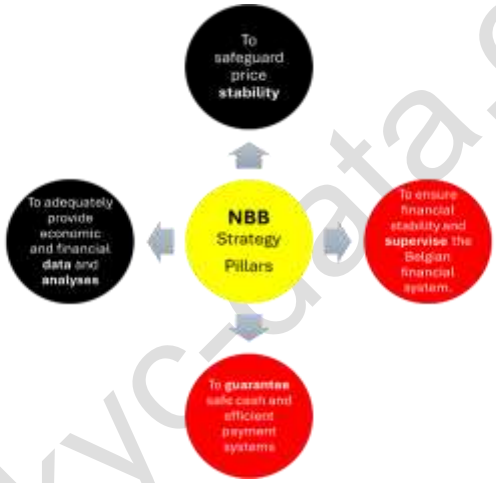
Belgium

Commentary

Financial Regulatory Authority

https://www.nbb.be/en (i)
https://www.nbb.be/en/about-national-bank/missions-and-strategy/four-missions-nbb (ii)
https://www.nbb.be/en/about-national-bank/administration-and-control/legal-framework (iii)
https://www.nbb.be/en/monetary-policy/general-framework/institutional-framework-monetary-policy (iv)

The National Bank of Belgium (**NBB**) serves as the central bank and regulator of the country. It has adopted a strategy which focusses on four core functions and activities as published on the NBB website.



(i)

Figure 7 The four pillars NBB strategy

Both Macro-prudential and Micro-prudential measures are used in terms of financial and economic analyses and policy implementation.

(ii)

Relevant legislation has been used to reflect the history and establishment of the NBB; with the most important being the Act of 22 February 1998 establishing the Organic Statute of the National bank of Belgium. In Chapter 1 of the Act the NBB is described as having been established originally by the Act of 5 May 1850 and under Article 2 forms a vital part of the European System of Central Banks. As a member of the ESCB, it must adhere to the relevant statute and protocols outlined in the Treaty of the Functioning of the European Union.(**TFEU**).

(iii)

Outlined on the NBB's website under the Monetary Policy heading there is a detailed insight into the institutional framework of monetary policy which the NBB follows. Following the signing of the Maastricht Treaty in 1999; there was a consensus to create an Economic and Monetary Union (EMU) involving member states. The EMU's monetary policy is conducted by the Euro System.

(iv)

Belgium's as a member of the EU has adopted the **euro**.

Commentary

AI Act / Policy

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0237 (i)

https://futurium.ec.europa.eu/en/european-ai-alliance/pages/about?language=en (ii)

Currently there are no laws which dictate AI governance and regulation in Belgium. However, as a member state of the European Union, relevant EU legislation can aid in understanding the scope and detail of proposed regulations in the field of AI as they apply to European Member States.

The above link directs to EUR-Lex, the EU's legal database of statutes, directives and resources which contains the European Commission's Communication regarding Artificial Intelligence in Europe. In section 1 (Introduction) there is reference made to the Commission's proposals for a European Initiative on AI, with the following tenets:

1. To focus on enhancing the technological and industrial capacity of AI uptake across the economy both from entities in both the private and public sector
2. Prepare for the socio-economic changes brought on by the uptake of AI including the modernisation of education and training systems, adaptation of social protection systems and considering changes made to the labour market
3. Devise and consolidate an appropriate ethical and legal framework, which reflects the Union's values in line with the Charter of Fundamental Rights of the EU

(i)

In term of ethical considerations regarding AI and the uptake of AI, the EU operates and maintains a forum for dialogue relating to the legal and ethical considerations of AI as well as other factors such as those social and economic in nature pertaining to Artificial Intelligence regulation. The URL connects to the European AI Alliance page of the European Commission's website.

(ii)

	Commentary
Anti-Money Laundering	https://www.nbb.be/en/financial-oversight/combating-money-laundering-and-financing-terrorism/information-and-19#at-the-national-level (i) https://www.nbb.be/doc/cp/eng/2023/law_18_09_2017_en_update_02_2023_bnb.pdf (ii) https://diplomatie.belgium.be/en/policy/policy-areas/peace-and-security/corruption-money-laundering-and-financing-terrorism (iii) https://www.ctif-cfi.be/index.php/en/belgian-system/ctif-cfi (iv) The NBB's website contains guidance of the NBB's AML/CFT regime and the legislation governing anti-money laundering and terrorist financing supported by reference. (i) T**he prevention of money laundering and terrorist financing and on the restriction of the use of cash** law which outlines the legal requirements and obligations implementing measures of the EU Directive **2015/849** as well as the overarching obligation to efficiently managing and mitigating the relevant risks involving AML/CFT which can be defined at a regional level, a National Level as well as at the level of the obliged entity itself. (ii) For further information relating to Belgium's response to Corruption, Money Laundering and the Financing of Terrorism consult the Belgium's federal public service website. (iii) The Belgian Financial Intelligence Processing Unit (**CTIF-CFI**) is the administrative authority, established under the Law on the prevention of money laundering and terrorist financing and on the restriction of the use of cash 2017 (AML Law), responsible for processing and disseminating information with view to combating ML/TF. The CTIF-CFI is the link between the different players involved in combatting money laundering and terrorist financing (*Federal Public Services, supervisory, regulatory or disciplinary authorities, police, customs*). (iv)
Bribery	https://diplomatie.belgium.be/en/policy/policy-areas/peace-and-security/corruption-money-laundering-and-financing-terrorism Bribery and corruption in Belgium is governed by the Penal Code. **Article 246** of the Belgian code relates to bribery offences and is defined as follows; 1. (**s1**.) The offences relating to what constitutes passive bribery. 2. This act involves a person exercising public duties who solicits, accepts, receives either directly or indirectly a promise or advantage of any nature for himself or another to adopt any of the behaviours adopted in article 247 of the BCC. 3. (**s.2**) The offences relation to what constitutes active bribery. This act involves the proposing of an offer, promise or advantage of any nature either directly or through third parties to a person who exercises public duties, for the person or another person in order that the individual may adopt any of the behaviours entailed and completed in article 247 of the BCC. **Article 247** of the Belgian Criminal Code relates to bribery offences and details penalties, fines and prison time from the perspective of public officials and their public duties. **Article 248** of the Belgian Criminal Code relates to bribery offences relating to policing authorities and officers or a judicial police officer of member of the prosecution. **Article 249** of the Belgian Criminal Code relates to bribery offences involving an arbitrator.

	Commentary
Consumer Protection	https://www.eccbelgium.be/ (i) https://www.eccbelgium.be/about-ecc/what-ecc-net-can-do-for-you/quality-charter (ii) With regards to Consumer protection in Belgium, the key point of reference would be the '**ECC'** or the **European Consumer Centre Belgium**. It outlines the rights dictated to the individual regarding consumer protection and has a public tool to give direct access to information regarding lodging complaints against businesses as well as individuals. (i) The ECC operates within the ECC-Net with its full title being the 'European Consumer Centres Network'. EEC-Net comprises twenty-nine centres across all member states of the EU, Norway and Iceland. The chief objective is to provides information relating to cross-border issues involving the EU, Iceland, Norway and in doing so enhance consumer protection and confidence. Through providing information both free and confidential advice to the public individuals is knowledgeable about their position relating to their role as a consumer. The EEC also aids relating to cross-border and transnational consumer rights and complaint handling. Further information relating to the EEC-Net's Quality Charter can be found via the corresponding URL. (ii)
Cloud Policy	https://www.dataprotectionauthority.be/citizen/the-be-dpa-approves-its-first-european-code-of-conduct (i) https://eucoc.cloud/en/about/about-eu-cloud-coc (ii) In 2021, the Belgian DPA (Data Protection Authority) approved its first European Code of Conduct adopted transnationally within the European Union. The EU Cloud COC has the primary objective of establishing good data protection and practices for cloud service providers and involves greater protection-based policies regarding personal data. (i) The EU COC seeks also to incorporate and follow the obligations specified under GDPR Article 28; as well as devising a monitoring and supervisory framework through bodies such as SCOPE Europe which acts as an independent monitoring body seeking to provide assessment on a yearly basis. Further information about the EU Cloud Code of Conduct (**EU COC**) can be found on the following website. (ii)

	Commentary
Data / Privacy	https://gdpr-info.eu/art-5-gdpr/ (i) https://www.dataprotectionauthority.be/publications/act-of-30-july-2018.pdf (ii) There are two key laws which apply to the processing of personal data in Belgium, which are: 1. EU General Data Protection (**GDPR**) 2. The Act of 30 July 2018 on the protection of natural persons with regards to the processing of personal data Europe's GDPR Principles are set out in Chapter 2, **Articles 5-11** and listed below: 1. Personal data should be processed lawfully, fairly and in a transparent manner in relation to the data subject 2. Personal data should be collected for specified, explicit and legitimate purposes and not further processed in a manner contravening these purposes 3. Personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed 4. Personal data should be accurate and where necessary kept up to date 5. Personal data should be kept in a form which permits the identification of data subjects for a period no longer than is necessary for the purposes for which the personal data are processed 6. Personal data should be processed in a manner which ensures appropriate security of the personal data (i) It is important to note that under Article 4 of the **Introductory Provisions of the Belgian DPA's** publication applies to the processing of personal data in the context of activities of an establishment of a controller or processor established on Belgian territory, whether the processing is performed in Belgian territory. However, under Chapter 3 ('Rights of the Data Subject') s.2, there is also an obligation for the controller to facilitate the exercise of the data subject's rights by virtue of articles 35 and 38 to 41 and as a member state of the EU, Belgium must adhere to the standards and protocols outlined by the relevant EU legislation as well as its own national laws. (ii)
Fraud	https://www.fsma.be/en/warnings/companies-operating-unlawfully-in-belgium For a list of companies operating unlawfully in Belgium, please consult the following list – this may include but is not restricted to fraudulent activity which contravenes the FSMA guidelines. The list is not exhaustive but involves those who act without due consideration and inevitably transgress the legislation regarding financial services in Belgium.
Sanctions	https://finance.belgium.be/en/about_fps/structure_and_services/general_administrations/treasury/financial-sanctions/national (ii) The Belgian National list of terrorist suspects whose assets have been frozen. The General Administration of the Treasury maintains an up-to-date, consolidated list of persons and entities including national, European and International lists.

Commentary	
Terrorism	https://finance.belgium.be/en/about_fps/structure_and_services/general_administrations/treasury/financial-sanctions/national (i) https://www.nbb.be/en/financial-oversight/combating-money-laundering-and-financing-terrorism/information-and-14#3-obligation-to-have-a-monitoring-system (ii) On the Belgian Federal Public Service (Finance) website is a national list of terror suspects whose assets have been frozen. This list follows Resolution 1373 (2001) of the Security Council of the United Nations which calls upon states to freeze the funds and economic assets of any person/s and entities who commit or attempt to commit acts of terrorism. Belgium has published a national terrorism list, in line with the guidance provided by the UNSC. (i) Further information about freezing measures and financial sanctions can be found in the NBB's website, using the link. It is important to note that by royal decree of 28 December 2006 there were relevant provisions made regarding restrictive measures against certain person/s entities involved in terrorism or the facilitation of terrorist activity, with these provisions ratified by Article 155 of the Law of 25 April 2007. Under the royal decree, funds and resources of an economic nature belonging to those on the national list are to be frozen. There is also a provision prohibiting both the direct and indirect availability of funds or financial resources to sanctioned persons or entities. (ii)
Company Registrar	https://economie.fgov.be/en/themes/enterprises/crossroads-bank-enterprises (i) https://economie.fgov.be/en/themes/enterprises/crossroads-bank-enterprises/services-everyone/consultation-and-research-data/cbe-public-search (ii) Users can access a wealth of company information for businesses in Belgium through their publicly available trade register. (i) CBE Public search offers a comprehensive search capability. (ii)
Access	https://transparencia.be/ The Transparencia platform helps citizens request access to information held by public authorities.
Other	https://www.belgium.be/en (i) https://www.federal-government.be/en (ii) Official Belgium information and services. (i) Federal Government website. (ii)

Posture Rating Belgium

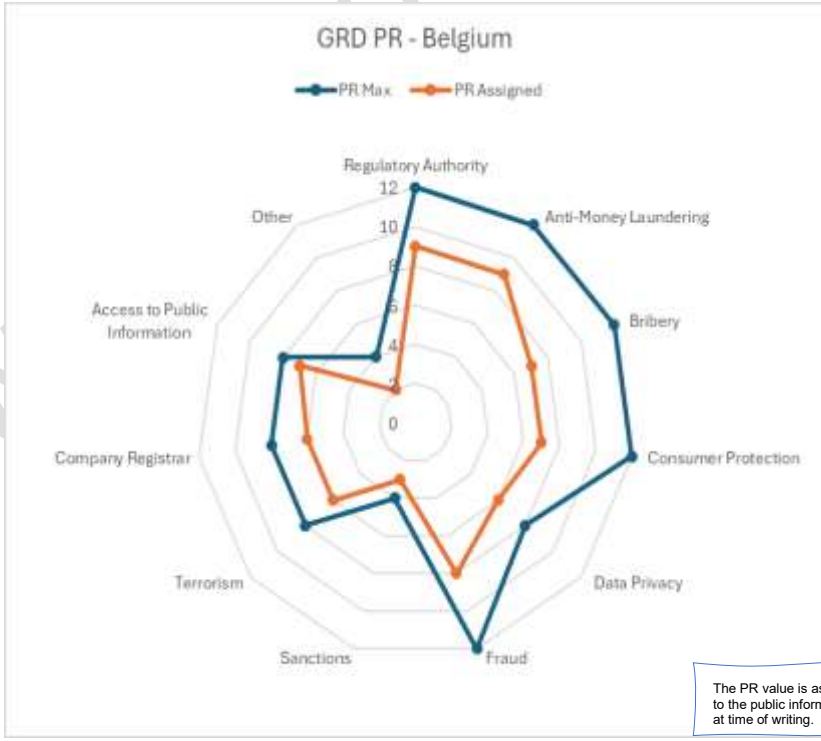
The PR value of **7.0** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	9	9	7	7	6	8	3	6	6	7	2

Belgium as a member of the EU, inherits many of the processes, regulations and laws to meet any domain obligations and has a high maturity level for its compliance regimes.

It should be noted that the Belgium adoption and promotion of the AMLD5 act is reflected in the overall AML Score.

NB: **The figure does not reflect the execution of any of these laws or regulations**.



The PR value is assigned subject to the public information available at time of writing.

Bermuda

Commentary

Financial Regulatory Authority

https://www.bma.bm/

The Monetary Authority (**BMA**) regulates & inspects Bermuda's financial institutions, issues currency, manages exchange control transactions & advises Bermuda's Government.

The three main goals of the BMA are as follows:

1. Maintain effective regulatory frameworks by cultivating a highly skilled and engaged workforce.
2. Deliver efficient operations and sustainable business practices.
3. Promote responsible innovation, both locally and in the global markets.

The national currency is the Bermudian **dollar.**

AI Act / Policy

https://www.gov.bm/articles/bermuda-hosts-successful-roundtable-discussion-advance-its-digital-asset-ecosystem

There are currently no specific laws in Bermuda regarding the use of AI.

Bermuda's Economic Development Department (**EDD**) held a round table discussion in 2013 with the aim of advancing Bermuda's digital asset ecosystem. AI was a key consideration in this discussion, with emphasis being placed on the need to strengthen AI regulation and enhance overall personal data protection in Bermuda.

Anti-Money Laundering

https://www.bma.bm/supervision-regulation (i)

https://www.bma.bm/legislation (ii)

In accordance with the **Proceeds of Crime Act 2008** (which came into effect in 2009), the **BMA** are the governing authority responsible for monitoring financial institutions and ensuring compliance with **AML/CFT regulations** in Bermuda.

The Proceeds of Crime Act, 2008 is one of the most significant pieces of legislation in relation to combatting money laundering. It replaced the **Proceeds of Crime act of 1998** broadening the scope of entities regulated under the law and introducing a **'risk-based AML/AFT'** system for all financial institutions to implement.

(i)

There are various other legislations pertaining to AML/CFT in Bermuda, all of which are available to download from the BMA website.

(ii)

Commentary

Bribery

https://www.bermudalaws.bm/Laws/Consolidated%20Law/2016/Bribery%20Act%202016 (i)

https://www.gov.bm/sites/default/files/BRIBERY-ACT-2016-Guidance-FINAL2.pdf (ii)

The most consequential piece of legislation in Bermuda with regards to tackling bribery is the **Bribery Act, 2016.** This act covers the following:

(i)

Bermuda's Ministry of Legal Affairs also issued a **guidance document**, aimed primarily at commercial organizations to help prevent bribery offences occurring in the workplace.

The 2016 Act replaced previous legislation on corruption, providing a more comprehensive framework for investigators and prosecutors when tackling bribery, both domestically and/or internationally. Furthermore, the Act strives to elevate Bermuda's international reputation, facilitating closer relations with the **UN Convention Against Corruption** and **OECD Anti-Bribery Convention.**

(ii)

Consumer Protection

https://www.bermudalaws.bm/Laws/Consolidated%20Law/1999/Consumer%20Protection%20Act%201999 (i)

https://www.gov.bm/department/consumer-affairs (ii)

In 1999, the Government of Bermuda issued its first official **Consumer Protection Act, 1999.** The main features of the act are as follows:

1. Establishing the **Consumer Affairs Board** and outlining their functions
2. Stipulating what constitutes as **unfair business practices**
3. General consumer safety requirements
4. **Powers of the Board** when enforcing consumer protection laws/regulations

(i)

The Government of Bermuda has a designated governing authority responsible for handling all matters concerning consumer protection- the **Department of Consumer Affairs.** Their duty is to supervise, monitor and regulate businesses who offer consumer goods and services, ensuring full compliance with the Consumer Protection Act of 1999.

(ii)

Cloud Policy

https://cdn.bma.bm/documents/2024-02-21-12-03-19-DAB-Operational-Cyber-Risk-Management-Code-of-Practice.pdf

Bermuda's cloud policy can be found enshrined within the BMA's **Digital Asset Business Operational Cyber Risk Management Code of Practice, 2024.** This stipulates that all cloud computing services must be risk-assessed in accordance with the type of cloud architecture. The risk assessment covers the following topics:

1. Governance and Enterprise Risk Management (**ERM**)
2. Legal issues
3. Compliance and audit
4. Information governance

Commentary

Data / Privacy

https://www.gov.bm/privacy-personal-information-protection-act-pipa (i)

https://www.gov.bm/sites/default/files/Personal-Information-Protection-Act-2016.pdf (ii)

In 2016, Bermuda released the Personal Information Protection Act (**PIPA**), due to fully come into force from 2025 onwards. The legislation is aligned with international best practices, applying to the State, businesses and all other organizations operating within Bermuda.

The main purpose of this legislation is to outline the requirements of organizations when collecting and processing personal information, along with outlining the rights of individuals regarding the use of their data.

The governing authority responsible for enforcing the act is the **Privacy Commissioner,** an independent body whose main duties are to ensure compliance with the PIPA and educate organizations and the public on matters concerning data privacy.

(i)

The full document is available to download as a PDF from the Government of Bermuda website.

(ii)

Fraud

http://parliament.bm/admin/uploads/bill/e6354d98ac533c52f61140ba0760d6ac.pdf

The Government of Bermuda issued the **Fraud Act 2017**; a comprehensive framework for businesses and individuals within Bermuda aimed at combatting fraudulent activity and outlining penalties in place for convicted offenders.

As a British Overseas Territory, the 2017 act closely aligns with the **United Kingdom's Fraud Act 2006** (with necessary modifications).

The act was introduced to modernise Bermuda's legislation on fraud, with one of the defining features being the creation of a **new general offence of fraud.** This highlights three possible ways of committing fraud, enshrined within clauses **4,5 and 6** of the Act.

Sanctions

https://www.bma.bm/international-sanctions

The Ministry of Legal Affairs Financial Sanctions Implementation Unit (FSIU) provides important and current information related to sanctions for Bermuda.

Terrorism

https://www.bma.bm/viewPDF/documents/2023-11-08-14-07-43-Anti-Terrorism-Financial-and-Other-Measures-Act-2004.pdf (i)

https://www.gov.bm/sites/default/files/211118_AML-ATF_Advisory_3_2021_APPROVED.pdf (ii)

In 2004, the Government of Bermuda issued the **Anti-Terrorism (Financial and Other Measures) Act**. The main objective is to clearly define what classifies as terrorist financing and stipulate the powers of governing authorities when regulating against it.

(i)

Bermuda is a member of the **FATF** and as such, aligns their anti-terrorism strategy closely with recommendations made by the group. For example, in 2021, the **Ministry of Legal Affairs and Constitutional Reform** issued a ministerial advisory. This introduced a new requirement of **enhanced customer due diligence** for jurisdictions deemed to be at **high risk** of money laundering or terrorist financing by the FATF or Caribbean Financial Action Task Force (**CFATF**).

(ii)

Commentary

Company Registrar

https://www.gov.bm/department/registrar-companies (i)
https://www.registrarofcompanies.gov.bm/bmroc-master/viewInstance/view.html?id=61bf8f1804cf9999fad0e50f613d82e89811ebb0eabd4bae&_timestamp=2815419706538738 (ii)

The Office of the Registrar of Companies (**RoC**).

(i)

Registered users can also search entities and reserved names in Bermuda via the RoC website.

(ii)

Access to Public Information

https://www.gov.bm/public-access-information-pati

The Government of Bermuda has a page on its official website dedicated to Public Access to Information (**PATI**).

All Bermudian citizens have the right to request public information from the relevant authorities, although may be required to pay a fee to obtain the requested records.

Other

https://www.gov.bm/ (i)
https://www.gov.bm/sites/default/files/PATI_Pati_statement_ITO.pdf (ii)

The official website providing government information and services.

(i)

Bermuda Government - Department of Information and Digital Technologies (IDT) note.

(ii)

Posture Rating Bermuda

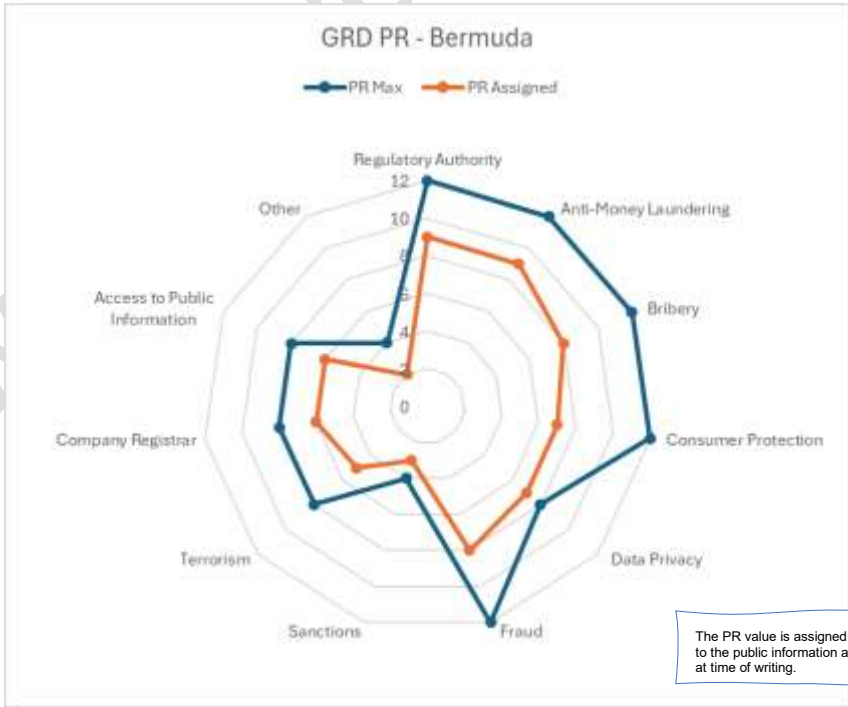
The PR value of **7.0** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	9	9	8	7	7	8	3	5	6	6	2

Bermuda has adopted processes, regulations and laws to support its domain obligations.

Whilst we did in some circumstances observe a lack of digital channels for some domains , we did observe the pattern of investment to foster the international reputation of Bermuda per domain and allocated the values accordingly.

NB: **The figure does not reflect the execution of any of processes, laws or regulations**.



Brazil

Commentary

Financial Regulatory Authority

https://www.bcb.gov.br/en/about/cmnen (i)
https://www.bcb.gov.br/en (ii)
https://www.bndes.gov.br/SiteBNDES/bndes/bndes_en/ (iii)

The National Monetary Council (**CMN**) is the major institution of the National Financial System (**SFN**) of Brazil and oversees the formulation of monetary and credit policies, aiming to preserve Brazilian monetary stability and to promote economic and social development and is composed of three members, each with a vote in every deliberation.

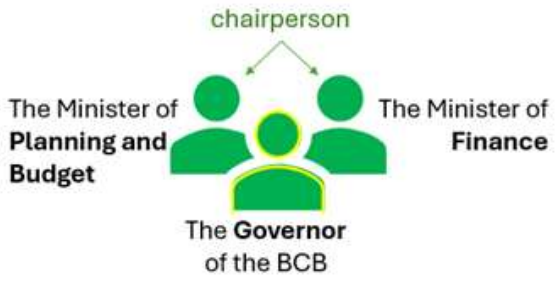


Figure 8 Composition of the Brazilian CMN

(i)

The Banco Central do Brasil (**BCB**) is the Central Bank of Brazil and performs its functions as a *monetary, regulatory and supervisory* authority in accordance with guidelines issued by the CMN. The mission of BCB, as with many other central banks is to ensure:

1. Stability of the currency purchasing power
2. Foster a sound, efficient and competitive financial system
3. Promote the economic well-being of society

(ii)

The Brazilian Development Bank (**BNDES**) is the main financing agent for development in Brazil and offers financial support mechanisms to Brazilian companies of all sizes as well as public administration entities, enabling investments in all economic sectors.

(iii)

The Brazilian **real** (BRL) is the official currency of Brazil.

Commentary

AI Act / Policy

https://www.gov.br/cnpq/pt-br (i)

https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ebia-summary_brazilian_4-979_2021.pdf (ii)

Currently there is no specific national legislation to regulate AI in Brazil, however some applicable legislation exists relevant to AI especially in the domain of data protection.

The Brazilian National Council for Scientific and Technological Development (**CNPq)** is governed by the Ministry of Science and Technology, dedicated to the promotion of scientific and technological research and to the formation of human resources for research in the country.

(i)

The Brazilian Artificial Intelligence Strategy (**EBIA**) was issued in 2021 and during July 2024 the Brazilian government's unveiled a 23 billion reais proposal for an AI investment plan aimed at developing sustainable and socially oriented technologies.

(ii)

Anti-Money Laundering

https://www.bcb.gov.br/en/financialstability/moneylaundering (i)

http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacao-em-ingles/law-9-613-anti-money-laundering-law/view (ii)

The Brazilian regime for anti-money laundering/combating the financing of terrorism (AML/CFT) is cantered at the Council for Financial Activities Control (**Coaf**)—the Brazilian financial intelligence unit. Coaf is entrusted with technical and operational autonomy however is administratively linked to the BCB.

(i)

Law No. 9,613/1998 (the 'AML Law') created Coaf and stablished a comprehensive framework of anti-money laundering requirements for a wide range of financial institutions.

(ii)

Bribery

https://www.oecd.org/en/about/news/press-releases/2023/10/brazil-must-make-urgent-key-reforms-to-build-on-its-recent-progress-in-the-fight-against-foreign-bribery.html

The Brazilian Clean Company Act, also known as the **Brazilian Anti-Corruption Act**, is a law that holds companies accountable for corrupt activities. The Brazilian Anti-Bribery Law (Law **No. 12,846/2013**) establishes judicial and administrative sanctions for legal entities.

It should be noted that if the bribe is committed in Brazil, then individuals will be subject to **criminal** sanctions whilst Brazilian companies will be subject to **civil** sanctions.

OECD posting referencing how Brazil must make urgent key reforms to build on its recent progress in the fight against foreign bribery.

Commentary

Consumer Protection

https://www.gov.br/mj/pt-br/assuntos/seus-direitos/consumidor/Anexos/guia-do-consumidor-estrangeiro-ingles.pdf

The Consumer Protection Code (**CDC**) governs all commercial relationships in Brazil, establishing rights and obligations for both consumers and suppliers. The CDC was enacted in 1991 and amended in 2013 to address the growing number of online transactions.

The CDC (Federal **Law No. 8,078/1990**) is often referred to as the Brazilian Consumer Defence Code and the URL above is the document distributed by the Ministry of Justice to explain consumer rights.

Cloud Policy

https://www.gov.br/anpd/pt-br/assuntos/noticias/resolucao-normatiza-transferencia-internacional-de-dados (i)

https://www.bcb.gov.br/content/about/legislation_norms_docs/BCB_Resolution_No_85_2021.pdf

There is no exclusion to using cloud services under regulatory laws, however there are several controls which need to be observed when contracting for the provision of Cloud services for an entity registered in Brazil, such as compliance to the LGPD.

During August 2024 the Autoridade Nacional de Proteção de Dados, published its long-awaited **International Data Transfer Regulation**. See “ANPD approves regulation on international data transfers”.

(i)

The National Monetary Council (**CMN**) Resolution **No. 4,893** provides for *cyber security policy and requirements for data processing and storage and cloud computing services to be followed* by financial institutions and similar entities.

The Central Bank ("**BCB**") Resolution **No. 85** regulates matters with respect to payment institutions and sets forth requisites for processing and storing data and for cloud computing solutions for information collected by financial institutions.

(ii)

Additionally, Brazilian Securities and Exchange Commission ("**SEC**") Resolution **No. 35**,establishes rules and proceedings to be followed in respect of the intermediation of securities on regulated securities markets by the entities under its supervision.

Data / Privacy

http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm

The **LGPD** (Lei Geral de Proteção de Dados Pessoais) is the federal data privacy law that governs all personal data processing within Brazil. It was passed in August 2018 and took effect in August 2020.

The LGPD grants the Brazilian National Data Protection Authority (“**ANPD**”) authority to establish a set of minimum technical standards to be implemented by controllers and processors.

Brazilian law permits international data transfers when the third country provides an adequate level of protection comparable to the LGPD.

Commentary

Fraud

https://www4.planalto.gov.br/legislacao

Brazil has several laws that address fraud and corruption, including:

1. **Criminal Code** - Includes provisions that criminalize fraudulent appropriation and fraudulent misrepresentation.
2. **Clean Company Act** - holds companies liable for corruption and bribery committed by their employees, officers, directors and shareholders. It applies to both domestic and foreign companies operating in Brazil.
3. **Law 7,492/1986** - Punishes fraudulent and reckless management of financial institutions with imprisonment and fines.
4. **Law 14,478/2022** - Includes virtual assets service providers in the definition of financial institutions. It also includes fraud in services involving virtual assets, securities, or financial assets as a crime.
5. **Law No. 14.155** - addresses theft committed through fraud using an electronic device with imprisonment and fines.

Sanctions

https://portaldatransparencia.gov.br/sancoes/consulta?cadastro=1&ordenarPor=nomeSancionado&direcao=asc

Federal Government Transparency Portal with Sanctions for;

1. Disreputable and Suspended Companies *(Hourly Update)*
2. Non-Profit Entities Prevented *(Daily Update)*
3. Companies Punished *(Hourly Update)*
4. Leniency Agreements *(Hourly Update)*

Terrorism

https://www.bcb.gov.br/en/financialstability/financialcrimes

Banco Central do Brasil is responsible for supervising the compliance by all supervised entities with the provisions of **Law 9,613/1998**, which provides on prevention of money laundering and terrorism funding in the National Financial System (SFN).

Company Registrar

https://www.in.gov.br/en/web/dou/-/instrucao-normativa-drei/sgd/me-n-82-de-19-de-fevereiro-de-2021-304448972 (i)
https://www.b3.com.br/en_us/products-and-services/trading/equities/listed-companies.htm (ii)

The National Department of Business Registration and Integration maintains a company registry. (i)
B3 S.A. - Brasil, Bolsa, Balcão, previously known as BM&FBOVESPA, is one of the oldest stock exchanges in Brazil, located in São Paulo. (ii)

Access to Public

https://www.gov.br/acessoainformacao/pt-br

Government website to request and access information.

Other

https://www.gov.br/planalto/en/

The official Brazilian Governmental website.

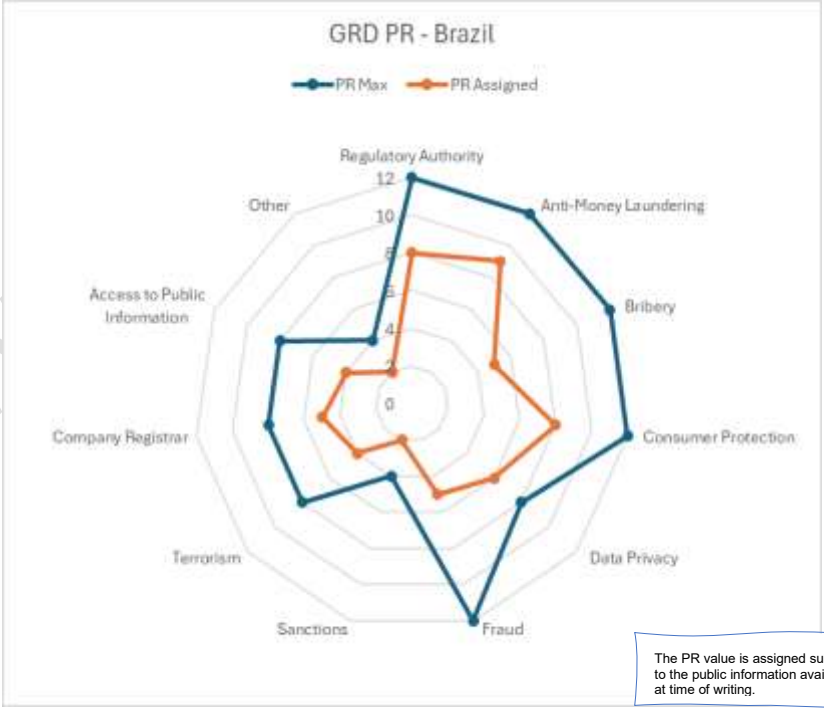
Posture Rating - Brazil

The PR value of **5.8** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	8	9	5	8	6	5	2	4	5	4	2

Brazil has introduced several, regulations and laws to address and define compliance obligations for the domains. However, we observed several weaknesses especially in the process for reporting bribery and the lack of digital channels to support the domain.

NB: **The figure does not reflect the execution of any of processes, laws or regulations**.



Brunei Darussalam

Commentary

Financial Regulatory Authority

https://www.bdcb.gov.bn/ (i)
https://cms.bdcb.gov.bn/storage/uploads/publications/17089426538595660.pdf (ii)
https://www.bdcb.gov.bn/monetary-policy/monetary-policy-framework (iii)
https://bdif.com.bn/ifb-public/front/ (iv)

Brunei Darussalam Central Bank (**BDCB**) is the financial regulatory authority for Brunei Darussalam with the following objectives :

1. To achieve and maintain domestic price stability
2. To assist and oversee the functioning of efficient payment systems
3. Formulating financial regulations and prudential standards to ensure the stability of the financial system
4. To foster and develop a sound and progressive financial services sector

(i)

Since 1967, the Brunei Dollar has been pegged to the Singapore Dollar under the Currency Interchangeability Agreement (**CIA**). This essentially means that the monetary authorities and banks of both countries must 'accept and exchange each other's currencies at par without charge and in their own currency'.

(ii)

The BDCB's monetary system is centred around the ***Currency Board Arrangement***, which was formed because of the CIA. This arrangement means that the Singapore dollar anchors the Brunei dollar and additionally, monetary policy decisions made by the Monetary Authority of Singapore (**MAS**) directly influence monetary conditions in Brunei.

(iii)

Brunei Darussalam Islamic Finance (**BDIF**) is an initiative to support His Majesty the Sultan and Yang Di-Pertuan of Brunei Darussalam's aspirations to become an international hub for Islamic Finance.

(iv)

The national currency in Brunei is the Brunei **dollar.**

AI Act / Policy

https://aiti.gov.bn/regulatory/ai-governance-and-ethics/

The Government of Brunei has yet to publicly announce a national AI strategy and is still in its early stages of investing in AI.

In May 2024, the authority for Info-communications Technology Industry (**AITI**) established the AI Governance and Ethics Working Group; In July the group issued its first draft guidance document, directed towards organizations that design, develop and/or use AI in Brunei, focusing on its ethical implications and safe-guarding considerations.

The guide is a working document and hence will be amended periodically to adjust to the ever-changing AI landscape.

Commentary

Anti-Money Laundering

https://www.agc.gov.bn/AGC%20Images/LAWS/ACT_PDF/cap209.pdf

In 2011, the Government of Brunei issued its revised edition of **Chapter 209** of the **Laws of Brunei- Anti Money-Laundering**.

This act was primarily introduced to prevent Brunei's financial system being exploited for money-laundering purposes. The act provides a comprehensive framework for businesses, organizations and other financial entities, covering various topics, including:

1. Obligations of legal and natural persons in preventing and detecting money laundering and terrorist financing
2. Necessary procedures for screening, identification and verification of customers
3. Powers of relevant supervisory authorities

Bribery

https://www.agc.gov.bn/AGC%20Images/LAWS/ACT_PDF/CAP%20131.pdf (i)

https://www.acb.gov.bn/SitePages/Background.aspx (ii)

Brunei's legislation regarding bribery is enshrined within Chapter 131 of the Laws of Brunei- **Prevention of Corruption.**

(i)

In accordance with the **Prevention of Corruption Act** (Chapter 131), the Government of Brunei established an **Anti-Corruption Bureau.** This is an independent body whose duty is to enforce anti-corruption legislation as stipulated in the Prevention of Corruption Act.

(ii)

Consumer Protection

https://www.agc.gov.bn/AGC%20Images/LAWS/ACT_PDF/C/CHAPTER%20261.pdf (i)

https://deps.mofe.gov.bn/cad/Our%20Law%20-%20Consumer%20Protection.aspx (ii)

Chapter 261 of the Laws of Brunei i.e. the Consumer Protection (Fair Trading) Order (**CPTFO**) is the primary piece of legislation in Brunei relating to consumer protection.

(i)

The **Department of Economic Planning and Statistics** from the Ministry of Finance and Economy is the governing body responsible for enforcing the CPFTO.

The main purpose of the act is to protect consumers against unfair practices by sellers. It applies to any business or consumers in Brunei, providing there is a business to consumer **(B2C) transaction.**

Some of the key elements covered are as follows:

1. Deceiving or misleading consumers e.g. using a small print to conceal terms and conditions
2. Making false claims
3. Exploiting a consumer who may not be able to protect their own interests

(ii)

Commentary

Cloud Policy

https://cicc.or.jp/english/wp-content/uploads/230209-2Brunei.pdf (i)
https://unn.com.bn/unn-launches-bruneis-first-locally-hosted-commercial-cloud-service (ii)

In 2023, the Ministry of Transport and Info-communications issued Brunei's **National Digital Policies and Projects in the New Normal Era**.

Within this publication, they made a commitment to developing a cloud policy, focusing on the usage of cloud computing services and infrastructure managed by third-party providers who share infrastructure with multiple organizations and use the public internet.

(i)

As part of Brunei's national digital transformation, the Unified National Networks (**UNN**) launched its first locally hosted commercial cloud service- Infrastructure-as-a-service (**IaaS)**.

The UNN is a government-owned organization, responsible for serving Brunei's Digital Telecommunication. The main objective of launching the new cloud hosting service was to boost Brunei's global reputation, offering organizations across the world a 'secure, scalable and resilient' cloud computing service.

(ii)

Data / Privacy

https://www.egnc.gov.bn/Shared%20Documents/EGNC%20Policies/Data%20Protection%20Policy.pdf (i)
https://www.agc.gov.bn/AGC%20Images/LAWS/Gazette_PDF/2025/EN/S%201_2025%20[E].pdf (ii)

The E-Government National Centre (**EGNC**) issued Brunei's **Data Protection Policy**, most recently revised in 2015.

The policy was implemented with the aim of governing the collection, use and disclosure of data in Brunei, ensuring high standards of 'confidentiality, integrity and availability' are always maintained.

The scope of this regulation is broad, outlining the duties of the Government with regards managing personal data, whilst also addressing how all other relevant parties use, process and access data.

(i)

In 2025, the Authority of Info-communications Technology Industry of Brunei (AITI) issued a Personal Data Protection Order (PDPO), which aims to incorporate various international data protection frameworks, strengthening Brunei's data protection laws in the private sector.

(ii)

Commentary

Fraud

https://www.agc.gov.bn/AGC%20Images/LAWS/ACT_PDF/Cap.22a.pdf

Brunei's anti-fraud policies can be found enshrined within Chapter 22 of the Laws of Brunei - **Penal Code.**

The Penal Code covers a broad spectrum of fraudulent activities punishable by criminal law in Brunei. Some of these include:

1. Fraudulent deeds and dispositions of property
2. False statements/claims in court
3. Alterations to items for the purpose of personal gain e.g. intentionally creating/using counterfeit coins
4. Forgery of documents

Sanctions

https://www.bdcb.gov.bn/aml-cft/information-for-reporting-institutions

UN Security Council Resolutions relating to terrorism implemented in Brunei Darussalam.

To access the Consolidated List of designated persons.

Terrorism

https://www.agc.gov.bn/AGC%20Images/LAWS/Gazette_PDF/2011/EN/s045.pdf (i)
https://www.bdcb.gov.bn/Pages/combating-the-financing-of-terrorism-(cft)-matters.aspx (ii)

In 2011, the Constitution of Brunei Darussalam issued its **Anti-Terrorism Order**, a comprehensive framework designed to tackle terrorism from its core. (i)

The legislation covers the following:

- Outlining what classifies as a terrorist offence
- Processes for investigating offences
- Seizing, freezing and confiscating terrorist property

Obligations of relevant entities to share information and the rights of persons being reported. (ii)

Company Registrar

https://www.mofe.gov.bn/Divisions/about-registry-of-companies-and-business-names.aspx (i)
https://business.mofe.gov.bn/SitePages/OBR.aspx (ii)

The Registry of Companies and Business Names (ROCBN) was established in 1959. (i)

The company registry can be searched via the official Government of Brunei 'BusinessBN' website. (ii)

Access to Public

https://www.data.gov.bn/Pages/index.aspx

Public information can be accessed via Brunei's Government Data Portal.

Other

https://deps.mofe.gov.bn/SitePages/BDEBluePrint.aspx (i)
https://www.gov.bn/SitePages/Home.aspx (ii)

The Economic Blueprint (issued in 2020) articulates six aspirations that form part of the nation's vision for institutional reforms and economic prosperity. (i)

The official website of the Government of Brunei Darussalam. (ii)

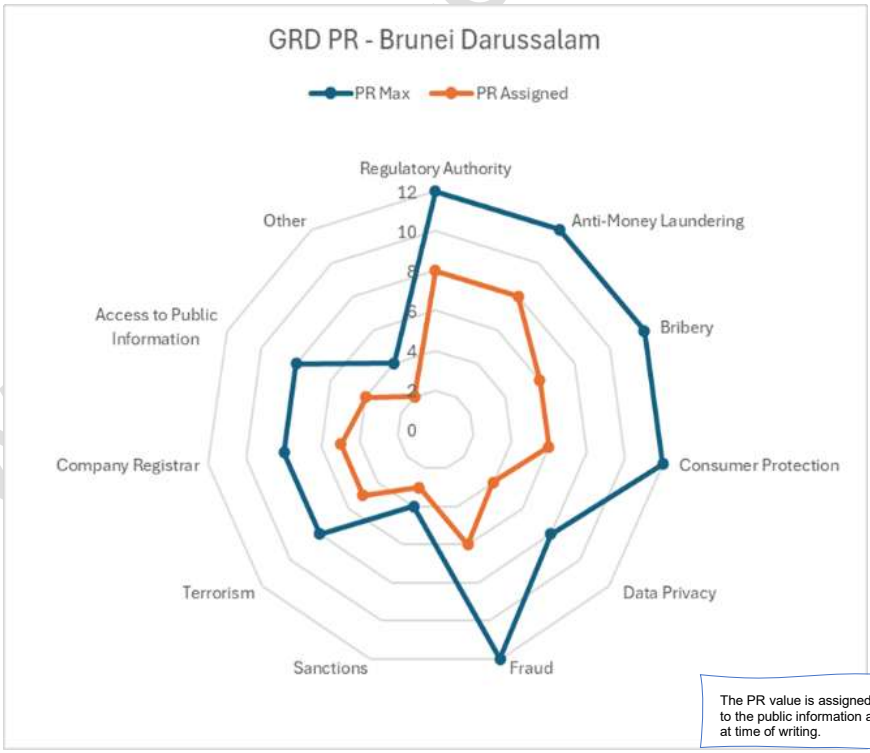
Posture Rating Brunei Darussalam

The PR value of **5.7** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	8	8	6	6	4	6	3	5	5	4	2

Brunei has introduced, regulations and laws to meet and define its compliance obligations, however we observed possible weaknesses regarding the Currency Interchangeability Agreement.

NB: **The figure does not reflect the execution of any of processes, laws or regulations**.



The PR value is assigned subject to the public information available at time of writing.

Republic of Bulgaria

Commentary

Financial Regulatory Authority

https://www.bnb.bg/index.htm (i)
https://www.fsc.bg/za-komisiyata/za-nas/ (ii)

The Bulgarian Nation Bank (**BNB**) has since 1st January 2007 been participating in the European System of Central Banks (**ESCB**).

(i)

The BNB is an independent emission institute of the state, which reports to the National Assembly. It has a key role in the Bulgarian economy and takes care of maintaining the sustainability of the Bulgarian currency, as well as strengthening and developing the country's banking and credit system.

As of 1997, Bulgaria joined a **currency board arrangement** i.e. assigning all responsibility to the BNB with regards to Bulgaria's monetary policy to help ensure price stability within the economy. There are various provisions under this arrangement, including:

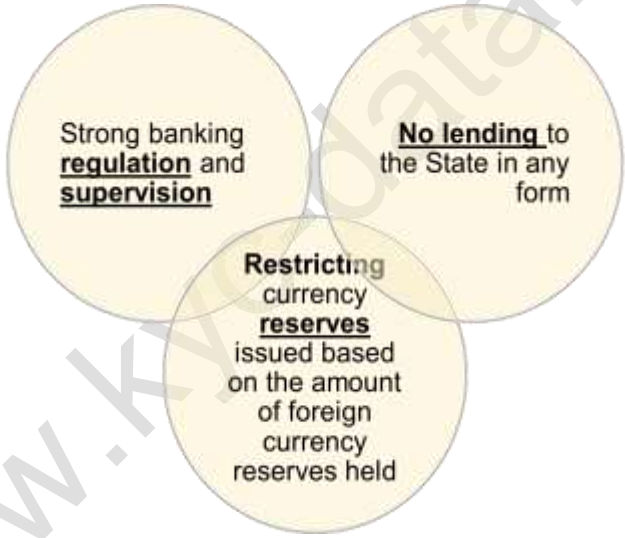


Figure 9 Three Core Provisions under the Bulgarian Currency Board Arrangement

The Financial Supervision Commission (**FSC**) is the governing body responsible for regulating the **non-banking financial system** in Bulgaria. Their main duties are to ensure stability and transparency in the financial sector whilst protecting the interests of investors, insurers and insured persons.

(ii)

The national currency in the Republic of Bulgaria is the **Bulgarian lev.**

Commentary

AI Act / Policy

https://www.mtc.government.bg/sites/default/files/conceptforthedevelopmentofaiinbulgariauntil2030.pdf (i)

https://www.mig.government.bg/wp-content/uploads/2022/12/isis-2021-2027.pdf (ii)

In 2021, the Ministry of Transport, Information Technology and Communications released Bulgaria's 10-year AI strategy- **Concept for the Development of Artificial Intelligence in Bulgaria until 2030.**

The main objectives of the strategy are as follows:

1. Create a reliable data infrastructure for the development of AI
2. Increase AI research capacity
3. Support innovation to implement AI in practice
4. Raise awareness and build trust in AI across society
5. Build a comprehensive regulatory framework for the use and development of reliable AI, compliant with international regulatory and ethical standards (i)

As an OECD accession candidate, Bulgaria also incorporates the OECD's AI principles into its policies. For example, the **Innovation Strategy for Smart Specialisation 2021-2017,** issued by the Ministry of Innovation and Growth, addresses four key OECD AI principles:

1. Inclusive growth, sustainable development and well-being
2. Investing in AI and research and development (R&D)
3. Cultivating a digital ecosystem for AI
4. Creating a stable policy environment for AI

Full strategy available to download as a pdf from the Government website. (ii)

Anti-Money Laundering

https://www.minfin.bg/en/1480 (i)

https://www.dato.bg/docs/Measures_Against_Money_Laundering_Act-%20%D0%97%D0%B0%D0%BA%D0%BE%D0%BD%20%D0%B7%D0%B0%20%D0%BC%D0%B5%D1%80%D0%BA%D0%B8%D1%82%D0%B5%20%D1%81%D1%80%D0%B5%D1%89%D1%83%20%D0%B8%D0%B7%D0%BF%D0%B8%D1%80%D0%B0%D0%BD%D0%B5%D1%82%D0%BE%20%D0%BD%D0%B0%20%D0%BF%D0%B0%D1%80%D0%B8.pdf (ii)

As an EU Member State, Bulgaria's anti-money laundering legislation is largely driven by various **EU Directives** (full list available on Bulgaria's Ministry of Finance Government website).

(i)

The Government of Bulgaria issued the **Measures Against Money Laundering Act, 2018** (most recently revised in 2022). This outlines measures for preventing money laundering occurring within the financial sector, clearly stipulating the powers and responsibilities of obliged entities e.g. the BNB and the FSC.

The key elements covered in the act are as follows:

1. Types of customer due diligence
2. Record retention and statistics
3. Disclosure of information
4. Protection of information and persons
5. National and international cooperation in tackling money-laundering
6. Penalty provisions (ii)

Commentary

Bribery

https://www.mfa.bg/en/bg-oecd (i)
https://www.oecd.org/en/topics/sub-issues/fighting-foreign-bribery/bulgaria-country-monitoring.html (ii)

Bulgaria became an OECD accession candidate in 2022. (i) As such, their approach to tackling bribery is largely influenced by the **OECD Working Group on Bribery's** recommendations.

In accordance with the OECD's phase 4 follow-up report- **Implementing the OECD Anti-Bribery Convention in Bulgaria**, the country has implemented various measures to combat bribery. These include:

1. Successfully implementing **15 of the OECD's 52 recommendations** (and partially implementing 19 of them)
2. Introducing the **Law on Whistleblowers**, helping to improve investigation and prosecution procedures with regards to bribery-related offences
3. Enhanced data collection and reporting of bribery-related offences to the Financial Intelligence Unit (**FID-SANS**)
4. Setting up a **Working Group** within the Ministry of Justice responsible for addressing phase 4 recommendations

The full report is available to download as a PDF from the OECD website.

(ii)

Consumer Protection

https://psc.egov.bg/en/user-guide-costomer-protection (i)
https://www.cem.bg/files/1654782793_consumer_protection_act.pdf (ii)

The Commission for Consumer Protection (**CCP**) is the governing body responsible for implementing and enforcing consumer protection legislation in Bulgaria.

The CCP's main duties include:

1. Monitoring the market for dangerous goods
2. Regulating against unfair commercial practices
3. Removing unfair terms in consumer contracts
4. Resolving disputes and imposing sanctions where necessary
5. Acting as an intermediary between Bulgaria and the EU regarding product safety

(i)

In 2005, the CCP issued the **Consumer Protection Act** (most recently amended in 2018). The main objectives of this act are to regulate the following:

- Protection of consumer's rights
- Powers and responsibilities of state authorities
- The activities of consumer associations

(ii)

Commentary

Cloud Policy

https://www.mtc.government.bg/sites/default/files/digital_transformation_of_bulgaria_for_the_period_2020-2030_f.pdf

In 2020, the **Digital Transformation of Bulgaria for the Period 2020-2030** was released. The aim of this publication was to increase the competitiveness of the Bulgarian economy by harnessing the full potential of digital technologies, including cloud computing.

One of the primary goals of this 10-year strategy is to increase the deployment of secure digital infrastructure, such as cloud computing, with the aim of improving both data security and scalability when implementing new technologies.

Data / Privacy

https://cpdp.bg/en/rules-on-the-activity-of-the-commission-for-personal-data-protection-and-its-administration/ (i)

https://cpdp.bg/en/legislation/personal-data-protection-act/ (ii)

The Personal Data Protection Act (**PDPA**) was first issued in 2002 (most recently revised 2023). The primary purpose of the act is to ensure the protection of natural persons regarding the processing of their personal data, pursuant to EU regulation.

Some of the key elements of the act are as follows:

1. Establishing the responsibilities of the Commission of Personal Data Protection (**CPDP**), including facilitating the free flow of personal data within the EU
2. Powers of the Supreme Judicial Council
3. Common rules concerning the processing of personal data and special cases
4. Stipulating the rights of natural persons and data subjects
5. Transferring of personal data to third countries or international organizations
6. Penalty provisions (i)

The CPDP is an independent supervisory authority, responsible for implementing the Personal Data Protection Act (**PDPA)** and ensuring Bulgaria is fully compliant with the EU General Data Protection Regulation (**GDPR)**. (ii)

Fraud

https://www.afcos.bg/sites/default/files/uploads/docs/2022-04/BULGARIAN%20NAFS_eng.pdf

The Government of Bulgaria released its National Strategy for Preventing and Combatting Irregularities and Fraud Affecting the Financial Interests of the European Union, due to be implemented over the period 2021-2027.

The primary aim of the strategy is to tackle fraud, corruption and other illegal activities impacting both Bulgaria's national finances and the finances of the EU.

The publication is fully aligned with EU initiatives, setting out four **key strategic goals** to help eradicate financial irregularities and fraud:

1. Better prevention e.g. policy on combatting conflict of interest
2. More effective fraud detection processes e.g. generalising the use of data analytics tools
3. Focus on improving investigation of fraud and financial irregularities, establishing shorter and clear recovery procedures and streamlining national rules on sanctions
4. Enhanced Cooperation with the European Anti-Fraud Office (**OLAF**), competent EU institutions, EU Member States and more active involvement in developing EU policies

Commentary

Sanctions

https://www.mfa.bg/en/ministry/mission-principles

Bulgaria does not currently have an independent nation-al sanctions list. However, as a Member State of both the UN and the EU, Bulgaria is bound by their sanctions policies.

Terrorism

https://rm.coe.int/moneyval-2024-1-bg-5thround-1stenhfur/1680afca6a (i)
https://www.mfa.bg/en/3103 (ii)

As specified in the Council of Europe's First Enhanced Follow-up report, the Measures Against the Financing of Terrorism Act 2003 (most recently revised in 2021) is one of the primary legislations governing the financing of terrorism in Bulgaria.
(i)

Bulgaria's **Ministry of Foreign Affairs** have also implemented various measures to combat terrorism on a global scale. Some of these include:

1. Adopting new counter-terrorism legislation to aid the prosecution of foreign terrorist fighters
2. Implementing a National Strategy and Action Plan to Combat Radicalism and Extremism
3. New sanctions regimes in line with UNSC resolutions on counterterrorism (ii)

Company Registrar

https://portal.registryagency.bg/en/

The Registry Agency at the Ministry of Justice maintains a national administrative register known as the **BULSTAT** Register.

This serves as a unified record for commercial and non-profit legal entities.

Access to Public Information

https://www.mi.government.bg/file/2012/03/zdoi_en_02_2022.pdf (i)
https://data.egov.bg/ (ii)

The **Access to Public Information Act, 2000** (most recently revised in 2022), states that all Bulgarian citizens have the right to access public information, as well as the right to re-use public sector information.

(i)

Public information can be accessed via the Government of Bulgaria's official Open Data Portal.

(ii)

Other

https://egov.bg/wps/portal/egov/nachalo (i)
https://egov.government.bg/wps/portal/ministry-meu/home (ii)

The government services and information portal.

(i)

Ministry of eGovernment official website.

(ii)

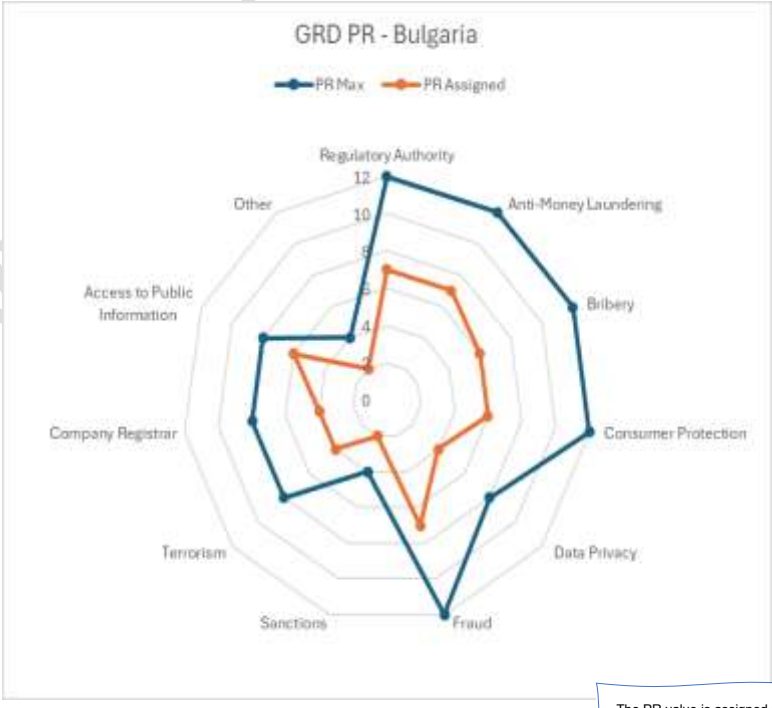
Posture Rating Bulgarian

The PR value of **5.5** has been derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	7	7	6	6	4	7	2	4	4	6	2

Bulgaria has introduced several, regulations and laws in synchronisation with the EU to meet and define compliance to its obligations. However, we observed several weaknesses in the online tools available to citizens which is reflected in the values assigned.

NB: **The figure does not reflect the execution of any of processes, laws or regulations**.



The PR value is assigned subject to the public information available at time of writing.

Canada

Commentary

Financial Regulatory Authority

https://www.bankofcanada.ca / (i)
https://www.canada.ca/en/financial-consumer-agency/corporate/federal-oversight-bodies-regulators.html (ii)
https://www.securities-administrators.ca/ (iii)
https://www.osfi-bsif.gc.ca/en (iv)

The primary financial regulator in Canada is the **Bank of Canada**.
The Bank's Council comprises the Governor, the Senior Deputy Governor and the Deputy Governors and has the responsibility to ensure the stability of the Canadian economy with the following areas of responsibility:

Figure 10 The Bank of Canada - Main Areas of Responsibility

(i)

The Government of Canada, while accountable, provides information on federal oversight bodies. However, each province and territory have their own regulatory bodies with the responsibility for overseeing financial institutions.

(ii)

The Canadian Securities Administrators (**CSA**) is the umbrella organization of Canada's provincial and territorial securities regulators whose objective is to improve, coordinate and harmonize regulation of the Canadian capital markets.

(iii)

The Office of the Superintendent of Financial Institutions (**OSFI)** is an independent agency of the Government of Canada with a mandate to regulate and supervise approx. 400 financial institutions and 1200 pension plans.

(iv)

AI Act / Policy

https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act (i)

https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document#s11 (ii)

In 2023, the Minister of Innovation, Science and Industry issued the **Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems.** This publication offers Canadian businesses and organizations a temporary framework containing common standards and ethical principles to abide by.

(i)

There is currently no specific regulatory framework in Canada relating to the systemic risks of designing and developing AI. Hence, Canda's Ministry of Innovation, Science and Industry, along with the support of the AI and Data Commissioner, are in the process of developing an Artificial Intelligence and Data Act (**AIDA**).

(ii)

Anti-Money Laundering

https://www.canada.ca/en/department-finance/programs/financial-sector-policy/canadas-anti-money-laundering-and-anti-terrorist-financing-regime-strategy-2023-2026.html (i)

https://fintrac-canafe.canada.ca/intro-eng (ii)

a. https://www.bankofcanada.ca/about/governance-documents/anti-money-laundering-and-anti-terrorist-financing-controls-framework/
b. https://lois-laws.justice.gc.ca/eng/acts/P-24.501/FullText.html
c. https://laws-lois.justice.gc.ca/eng/acts/C-46/section-462.31.html
d. https://www.fsrao.ca/
e. https://www.canada.ca/en/public-safety-canada/news/2022/12/financial-crimes-coordination-centre-co-leads-financial-action-task-force-report-on-money-laundering-from-synthetic-opioids.html

---

The outline for the Canadian Government's AML policy between 2023-2026.

(i)

Canada's financial intelligence unit (**FINTRAC**) oversees anti-money laundering and anti-terrorism financing.

The Bank has a team of specialists who use innovative technology to detect suspected financial crimes such as money laundering, terrorist financing and activities prohibited by sanctions. Their Financial Crimes Risk Management Program (**FCRM**) is periodically assessed for effectiveness.

a. The AML regime was established in Canada to combat money laundering and terrorist financing. It involved 13 agencies, including the RCMP, CBSA, CSIS and created the Financial Transactions and Reports Analysis Centre.
b. The Department of Finance and Public Safety Canada co-led the committee coordinating the regime's work
c. The AML-related Criminal Code and associated offences
d. The Financial Services Regulatory Authority (**FSRA**) is an independent agency that aims to enhance the province's consumer and pension plan protection. It has replaced FSCO and DICO and is a flexible, self-funded organization that can quickly adapt to changes in the market
e. FC3 is a 5-year initiative led by Public Safety Canada that brings together anti-money laundering experts from various jurisdictions to support

(ii)

Bribery

https://laws-lois.justice.gc.ca/eng/acts/c-45.2/page-1.html (i)
https://laws-lois.justice.gc.ca/eng/acts/c-36.65/ (ii)
https://laws-lois.justice.gc.ca/eng/acts/e-2.01/ (iii)
https://www.oecd.org/canada/ (iv)

Canada's anti-bribery legislation includes three key laws which are depicted below:

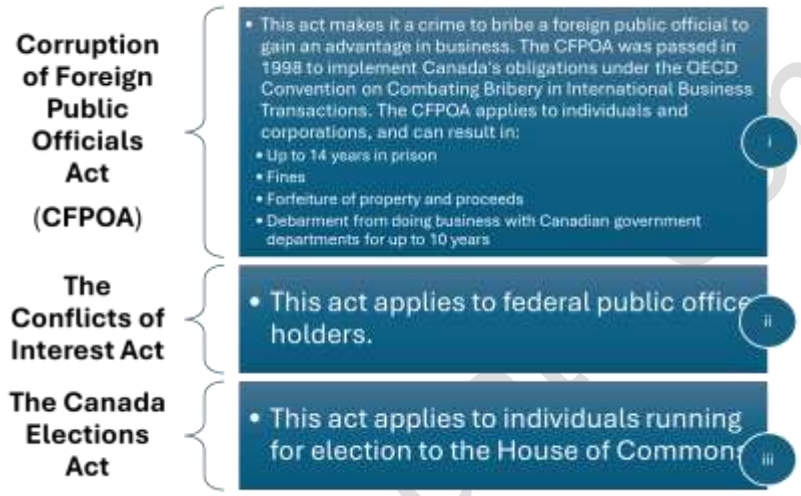


Figure 11 Canada's Anti Bribery Laws

It should be noted that *gifts, hospitality and other benefits* are acceptable to public officials if they're not part of contractual negotiations and follow all applicable laws and codes of conduct. The total value of any gifts received by a federal public official may need to be reported if it exceeds a certain threshold.

Canada joined the OECD Convention for Combating Bribery in International Business Transactions on December 17, 1997. In 1998, the Parliament passed the Corruption of Foreign Public Officials Act (**CFPOA**) to implement the convention into Canadian law.

(iv)

Fraud

https://fintrac-canafe.canada.ca/fa-af/1-eng (I)
https://www.canada.ca/en/services/finance/fraud.html (ii)
https://antifraudcentre-centreantifraude.ca/index-eng.htm (iii)
https://www.oag-bvg.gc.ca/internet/English/acc_rpt_e_42986.html#hd2b (iv)

FINTRAC has a fraud alert system that helps prevent scams and fraud. Unfortunately, people have misrepresented FINTRAC and its personnel to carry out their scams.

(i)

This website is the official platform for reporting fraud in Canada.

(ii)

The Canadian Anti-Fraud Centre gathers information on fraud and identity theft and offers resources on current and previous scams.

(iii)

The OAG follows the Fraud Risk Management Framework, which helps them identify, address and manage fraud risks by implementing best practices. (iv)

Commentary

Consumer Protection

https://ised-isde.canada.ca/site/office-consumer-affairs/en/federal-consumer-protection-legislation-canada (i)

https://laws-lois.justice.gc.ca/eng/acts/c-34/fulltext.html (ii)

https://www.canada.ca/en/financial-consumer-agency.html (iii)

https://ised-isde.canada.ca/site/office-consumer-affairs/en/federal-provincial-and-territorial-consumer-affairs-offices (iv)

There are numerous federal agencies in Canada that are responsible for enforcing legislation pertaining to consumer protection. These include:

1. The Canadian Radio-Television and Telecommunications Commission (CRTC)
2. The Competition Bureau
3. The Financial Consumer Agency
4. The Office of the Privacy Commissioner of Canada

(i)

The Competition Act, 1985 (last amended in 2024) is enforced by the Competition Bureau. The main objectives of this Act are as follows:

1. Promote efficiency and adaptability in the Canadian economy
2. Increase Canada's global standing
3. Ensure small and medium-sized businesses have equitable opportunity to participate in the economy
4. Provide competitive prices and product choices for consumers

(ii)

The **Financial Consumer Agency of Canada (FCAC)** is responsible for protecting consumer's rights and interests in relation to financial products and services.

(iii)

Further information about consumer protection can be requested from specific provincial and territorial consumer affairs offices across the country.

(iv)

Data / Privacy

https://laws-lois.justice.gc.ca/eng/acts/P-21/ (i)

https://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html (ii)

The Privacy Act of 1985 (last amended in 2024) aims to protect the privacy of Canadian citizens, ensuring they have the right to access information about themselves held by Government institutions. The Act covers the government's 'collection, use, disclosure, retention or disposal' of personal data.

(i)

The Personal Information Protection and Electronic Documents Act (**PIPEDA**) was issued in 2000 (last amended in 2024). The primary aim of this act is to stipulate how Canadian private-sector organizations should '*collect, use and disclose*' personal information. This also applies to the personal information of employees of federally regulated businesses.

(ii)

Cloud Policy

https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/cloud-adoption-strategy-2023-update.html (i)

https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/2024-application-hosting-strategy.html#toc-2 (ii)

https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/direction-secure-use-commercial-cloud-services-spin.html (iii)

https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/cloud-security-risk-management-approach-procedures.html (iv)

In 2023, the Government of Canada released the updated version of the Canadian 2018 **Cloud Adoption Strategy.**

The original strategy was implemented to address the **Cloud First** policy requirements**.** Subsequently the Government shifted its focus onto the principle of **Cloud Smart** i.e. still prioritising cloud as the preferred delivery model for IT services but not opting for 'cloud at all costs'

(i)

In 2024, the Government of Canada issued its **Application Hosting Strategy**. Similarly to the 2023 Cloud Adoption Strategy, this publication aims to improve the overall digital landscape and provision of digital services in Canada. As such, many Government agencies have optimised their use of cloud hosting, with the hopes of maximising business value, reducing technical debt and continuing to evolve the ever-growing service culture in Canada.

(ii)

The Treasury Board of Canada Secretariat (TBS) issued a Security Policy Implementation Notice (**SPIN**) in 2017 (modified in 2022).

The purpose of SPIN is to ensure departments understand existing TBS security requirements in relation to cloud computing and furthermore, outline guidance to support organizations in the secure use of commercial cloud services.

(iii)

The Government of Canada's **Cloud Security Risk Management Approach and Procedures** publication outlines the authorities, approach and procedures for managing security risks in the context of hosting using cloud computing services.

(iv)

Sanctions

https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/index.aspx?lang=eng (i)

https://laws-lois.justice.gc.ca/eng/acts/F-31.6/index.html

The Canadian Sanctions page on the Government website presents several valuable resources including the Canadian Sanctions Measures and a list of current sanctions.

(i)

Canadian sanctions are imposed under the:

1. United Nations Act (**UNA**);
2. Special Economic Measures Act (**SEMA**);
3. Justice for Victims of Corrupt Foreign Officials Act (**JVCFOA**)

In addition to sanctions imposed under the UNA, the SEMA and the JVCFOA, Canada has imposed measures against individuals under the Freezing Assets of Corrupt Foreign Officials Act.

(ii)

Terrorism

https://www.justice.gc.ca/eng/cj-jp/ns-sn/act-loi.html (i)
https://www.fatf-gafi.org/en/countries/detail/Canada.html (ii)
https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rslnc-gnst-trrrsm/index-en.aspx(iii)

Introduced in 2017, the Anti-Terrorism Act (**ATA**) aimed to improve the national security and safeguard Canadians' rights and freedoms.

The ATA has four key objectives, which are:

1. To protect the citizens of Canada from terrorist attacks by preventing terrorists from entering the country
2. Utilise tools to effectively identify, prosecute, convict and punish terrorists
3. Secure the Canada-US border
4. Collaborate with the international community in combatting terrorism, focusing on addressing the root causes of terrorist violence (i)

Canada has been a member of the **FATF** since 1990.

In 2021 Canada released a report detailing their efforts in implementing the FATF's recommendations. Based on this, the FATF concluded that Canada was fully compliant with 11 of the recommendations, mostly compliant with 23, partially complaint with 5 and non-compliant on one. (ii)

The Government of Canada released its **Counter-terrorism Strategy in 2012**. This sets out to assess the nature and scale of terrorist threats and outline the key foundational principles of the Government's counter-terrorism activities. (iii)

Company Registrar

https://www.canada.ca/en/services/business/research/directoriescanadiancompanies.html (i)
https://beta.canadasbusinessregistries.ca/search (ii)

The Directories of Canadian companies, allows one to Search business registries, check a company's incorporation status and find Canadian importers. (i)

Access to information from the official registries of Alberta, British Columbia, Corporations Canada, Manitoba, Nova Scotia, Ontario, Quebec and Saskatchewan. (ii)

Access to Public Information

https://laws-lois.justice.gc.ca/eng/acts/A-1/index.html (i)
https://www.canada.ca/en/parole-board/corporate/transparency/access-to-information-and-privacy/how-to-make-an-access-to-information-request.html (ii)

In 1985, the Government of Canada enacted the **Access to Information Act** (last amended in 2024). The purpose of the Act was to promote an open and democratic society, advancing trust and accountability in the federal institutions of Canada.

The Act also extends existing laws in Canada relating to the right of access to information and additionally, outlines the requirements for the positive publication of information. (i)

Citizens of Canada can submit an 'Access to Information Request' via the Government website. (ii)

Other

https://www.canada.ca/en.html (i)
https://www.canada.ca/en/employment-social-development/corporate/portfolio/service-canada.html (ii)

The official website of the Government of Canada (i)

Service Canada provides citizens with a single point to government services and benefits (ii)

Posture Rating - Canada

The PR value of **7.1** is obtained using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	9	8	8	7	6	8	3	6	6	7	3

Canada has introduced and matured regulations and laws to support the compliance of domain obligations assisted by digital channels.

NB: **The figure does not reflect the execution of any processes, laws or regulations**.

China (SAR) – Macau

Special Administrative Region of the People's Republic of China

Commentary

Financial Regulatory Authority

https://www.amcm.gov.mo/en/ (i)
https://www.amcm.gov.mo/en/about-amcm/history/amcm (ii)
https://www.amcm.gov.mo/en/about-amcm/history/the-pataca (iii)

The Macau Monetary Authority functions as a de facto central bank. It is responsible for maintaining the stability of Macau's financial system and for managing its currency reserves and foreign assets.

(i)

In accordance with its Statute the "Autoridade Monetária de Macau" (**AMCM**), the Issuing Institute of Macao (**IEM**) is the primary regulator of the financial sector in Macao. The IEM is responsible for regulating banking, insurance and other credit related activities.

(ii)

After the establishment of the AMCM, the authority to issue pataca was transferred to the Portuguese-administered Government.

The currency is 100% backed by foreign exchange reserves, pursuant to the AMCM currency board system.

(iii)

The **pataca** is the legal tender of the Macao Special Administrative Region (MSAR).

AI Act / Policy

Limited Information available at time of writing

Anti-Money Laundering

https://www.fatf-gafi.org/en/publications/Mutualevaluations/Mer-macao-2017.html (i)
https://www.gov.mo/en/news/118920/ (ii)
https://bo.io.gov.mo/bo/i/2006/14/lei02_cn.asp (iii)

Macau is an FATF member and as such, closely follows the **FATF's 40 recommendations** with regards to tackling money laundering.

(i)

In 2019, the Asia/Pacific Group on Money Laundering (**APG**) conducted a Mutal Evaluation Follow-up Report of Macau's AML/CFT activities. The feedback from the report was extremely positive, concluding that Macau had become the first member to pass all 40 FATF Technical Compliance Recommendations.

(ii)

Law No.2/2006- Prevent and deter money laundering crimes was enacted by the Legislative Council with the aim of supressing and preventing money laundering offences in Macau. Some of the key elements of the law include:

1. Criminal liability of legal persons
2. Special litigation measures
3. Obligations and powers of governing bodies
4. Precautionary provisions
5. Penalties

(iii)

Commentary

Bribery

https://www.ccac.org.mo/PrivSec/file/ch/en/ch3.pdf (i)
https://www.ccac.org.mo/PrivSec/en/law_details/article/kaz43wc3.html (ii)

In accordance with the principle of '*one country, two systems'*, Macau has its own independent legal system and judicial power.

The legal system closely aligns with European legislations.

In Macau, the anti-bribery provisions can be found enshrined in the **Penal Code** and the **Prevention and Suppression of Bribery in the Private Sector** law.

The Commission Against Corruption of Macau (**CCAC**) is the governing authority responsible for tackling bribery and corruption-related offences, both in the public and private sector. (i)

Law No.19/2009 – **Prevention and Suppression of Bribery in the Private Sector**. The objectives of this law are as follows:

1. Clearly stipulate what constitutes as bribery offences in the private sector
2. Outline a bribery prevention regime
3. Establish the powers of the CCAC (ii)

Consumer Protection

Only available in Portuguese or Chinese.

https://bo.io.gov.mo/bo/i/2021/28/lei09.asp (i)
https://bo.io.gov.mo/bo/i/2023/43/regadm38.asp (ii)

Law No.9/2021- **Law on the protection of consumers rights and interests** is the primary piece of legislation in Macau pertaining to consumer protection. The law aims to:

1. Establish a framework for protecting the rights and interests of consumers
2. Ensure the safety and quality of goods and services
3. Promote equality and justice in the legal relations between commercial operators and consumers
4. Increase transparency and tackle unfair commercial practices (i)

The **Consumer Advisory Council** was first established in 1988. They are the advisory body to the Government of the Macau Special Administrative Region, responsible for implementing policies and measures related to the protection of rights and interests of consumers.

(ii)

Cloud Policy

Limited Information available at time of writing

Fraud

https://www.ccac.org.mo/PrivSec/file/ch/en/ch3.pdf

Macau's anti-fraud policies are enshrined within the MSAR Government's **Penal Code**. Pursuant to Article 211, 'any person who seeks personal gain by fraudulent means and causes prejudice to another person's property shall be criminally liable.'

As with bribery, the **CCAC** are the governing body responsible for enforcing legislation pertaining to fraud offences.

Commentary

Data / Privacy

https://www.dspdp.gov.mo/file/Laws%20and%20Regulations/%E5%80%8B%E4%BA%BA%E8%B3%87%E6%96%99%E4%BF%9D%E8%AD%B7%E6%B3%95_TC.pdf (i)

Only available in Portuguese or Chinese

https://www.dspdp.gov.mo/en/company_profile.html (ii)

In 2005, the Macau Special Administrative Region (MSAR Government) issued its Personal Data Protection Act **(PDPA).** The main purpose of this act is to ensure all personal data processing is carried out transparently and respects the fundamental rights and privacy of the individual(s). The Act covers the following:

1. Processing and quality of personal data
2. Rights of the data subject
3. Security and confidentiality of processing
4. Transferring personal data outside of Macau
5. Obligations to notify relevant authorities

(i)

In 2007, the Office of Personal Data Protection (**OPDP**) was established and was later reformed, becoming the Personal Data Protection Bureau (**PDPB**).

The PDPB operates as a permanent public department for the MSAR Government (as opposed to a transitory project unit like the OPDP). Their mission is to ensure compliance with the PDPA and increase overall public awareness of personal data protection.

(ii)

Sanctions

https://www.ccrc.gov.mo/en_sanctionlists.html (i)

https://www.ccrc.gov.mo/en_about.html (ii)

The MSAR Government has adopted the **United Nations Security Council** sanction-related resolutions.

The full sanctions lists can be accessed via the Asset Freezing Coordination Commission's (**CCRC**) website.

The CCRC was established in accordance with Article 5 of **Law no.6/2016- Asset Freezing Regime**. The commission performs various functions, including;

1. Maintaining a public database with updated records on designated natural and legal persons, as well as frozen assets, in accordance with the UN Security Council Resolutions
2. Communicating with sanctioned entities and providing specific instructions to ensure compliance

(i)

Figure 12 Members of the Commission

(ii)

Commentary

Terrorism

Only available in Portuguese or Chinese

URL https://bo.io.gov.mo/bo/i/2006/15/lei03_cn.asp (i)
https://bo.io.gov.mo/bo/i/2006/20/regadm07_cn.asp (ii)

Language

In 2006, the Legislative Council of Macau enacted Law No.3- **Prevent and supress terrorist crimes**, in accordance with Article 71(1) of the Basic Law of Macau S.A.R. The law covers the following:

1. Defining the various forms of terrorism
2. Financing of terrorism
3. Criminal liability of legal persons
4. General and precautionary provisions

(i)

Administrative Regulation No.7/2006- **Preventive measures for money laundering and terrorist financing** was issued in accordance with the Article 50 (5) of the Basic Law of the Macau S.A.R. The purpose of this law is to outline the foundations of preventing money-laundering and terrorist financing crimes, along with setting up a system to monitor the compliance of obliged entities.

(ii)

Company Registrar

URL https://www.gov.mo/en/services/ps-1318/ps-1318b/ (i)
https://www.registrationchina.com/china-company-search/ (ii)

Official Government 'Registration for Controlled External Trade Operations - Company Registration' page.

(i)

URL to allow one to search the company registrar.

(ii)

Access to Public Information

N/A – No information available at time of writing

Other

URL https://www.gov.mo/en/ (i)
https://www.gov.mo/en/content/laws/constitutional-documents/ (ii)

Official website of the region.

(i)

Constitutional Documents.

(ii)

Posture Rating - Macau

The PR value of **5.2** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	8	7	6	6	6	7	2	5	3	0	2

It should be noted that at the time of writing there were 12 Banks incorporated in Macau and 20 Branches of banks incorporated overseas which in real terms makes supervision simple.

The Macau Special Administrative Region (**MSAR**) has several regulations and laws to address its legislative obligations.

Whilst information is available on the Registration for Controlled External Trade Operations webpage of the government company search is limited and is reflected in the PR Value.

In the absence on data available to us at the time of writing, relating to the availability of public information, we did not allocate a score which impacts the overall rating.

NB: **The figure does not reflect the execution of any processes, laws or regulations.**

Chile

Commentary

Financial Regulatory Authority

https://www.bcentral.cl/en/home (i)
https://www.bcentral.cl/en/web/banco-central/news-and-publications/normatives/summary-of-financial-standards (ii)
https://www.cmfchile.cl/portal/principal/613/w3-propertyvalue-26173.html (iii)

The Central Bank of Chile is the main financial regulator of Chile. It was established in 1925 and is incorporated into the current Chilean Constitution as an autonomous institution of constitutional rank.

The main objective of the Central Bank of Chile is to ensure currency stability.

The operating objective of the Central Bank of Chile is to maintain an annual inflation rate of around 3% over a horizon of about two years. The main instrument used to help achieve this objective is the **Monetary Policy Rate**, determined at each of the bank's Monetary Policy Meetings.

(i)

The Compilation of Financial Regulations.

(ii)

The Financial Market Commission (**CMF**) is responsible for regulating the Chilean Financial Market. The commission is affiliated with the President of the Republic of Chile through the Ministry of Finance. Their main objectives are as follows:

1. Ensure the correct functioning, development and stability of the financial market
2. Facilitate market agents' activities
3. Promote the protection of public trust (iii)

The national currency in Chile is the **peso.**

AI Act / Policy

https://minciencia.gob.cl/uploads/filer_public/bc/38/bc389daf-4514-4306-867c-760ae7686e2c/documento_politica_ia_digital_.pdf (i)
https://www.cepal.org/en/notes/ilia-2024-evaluating-ai-readiness-and-progress-latin-america (ii)

In 2021, the Ministry of Science, Knowledge, Technology and Innovation issued Chile's first **National Policy on Artificial Intelligence.**

The primary aim of this publication is to boost Chile's international standing with regards to AI by curating an 'ecosystem of research, development and innovation'.

The policy is underpinned by 4 transversal principals:

1. Human rights, security and well-being
2. Sustainable
3. Inclusive
4. Globalised and evolving

Chile is one of the countries categorised in the Latin American Artificial Intelligence Index (**ILIA 2024**). This index was jointly developed by the Economic Commission for Latin America and the Caribbean (**ECLAC**) and the National Centre for Artificial Intelligence of Chile (**CENIA)**.

According to the ILIA index, Chile is the leading country in the context of AI development, measured based on technological infrastructure, human talent development and AI governance frameworks.

Commentary

Anti-Money Laundering

https://www.cmfchile.cl/portal/principal/613/w3-article-55033.html (i)
https://www.fatf-gafi.org/en/countries/detail/Chile.html (i)
https://www.bcn.cl/leychile/navegar?idNorma=1195119&idVersion=2024-09-04&idParte= (iii)

In 2022, the CMF updated its regulation on the prevention of money laundering (ML), the financing of terrorism (FT) and non-proliferation of weapons of mass destruction. The regulation applies to banks (including subsidiaries and support companies), savings and credit cooperatives, payment card issuers.

The most consequential changes to the regulation in relation to preventing ML were as follows:

- Enhancing the identification process of the final beneficiaries
- Strengthening customer due diligence pursuant to a risk-based approach (i)

Chile is a Member State of the Financial Action Task Force of Latin America (**GAFILAT**) and hence many of the 2022 amendments to their National Strategy were made in accordance with the **FATF's 40 recommendations**.

(ii)

The **Economic Crimes Law, 2023** (most recently amended in 2024) also outlines provisions in place to strengthen Chile's anti-money laundering regulations, including enhanced compliance programmes and monitoring and reporting processes.

(iii)

Bribery

https://www.bcn.cl/leychile/navegar?idNorma=1984 (i)
https://www.oecd.org/en/topics/sub-issues/fighting-foreign-bribery/chile-country-monitoring.html (ii)

On a national level, Chile's **Penal Code, 1874** (most recently amended in 2022) stipulates specific provisions in place to combat bribery in Chile, with a particular focus on the bribery of public officials.

(i)

Chile is Party to the **OECD Convention on Combatting Bribery of Foreign Public Officials in International Business Transactions**. As such, their implementation of bribery-related legislation is heavily influenced by their recommendations and subject to rigorous monitoring and peer-review by the OECD Working Group on Bribery.

(ii)

Commentary

Consumer Protection

https://www.sernac.cl/portal/617/w3-channel.html (i)
https://www.sernac.cl/portal/618/w3-propertyvalue-59300.html (ii)
https://www.bcn.cl/leychile/navegar?idNorma=1170464 (iii)

The Consumer Protection Agency (**SERNAC**) is an autonomous supervisory authority, governed by the **Consumer Law (19,496).** Their mission is to protect consumer's rights in Chile from unfair business practices.

(i)

The Consumer Law aims to establish consumer's rights and clearly stipulate the obligations of companies. Some of the main issues it regulates are as follows:

1. Guaranteeing the right to truthful and timely information pertaining to goods and services
2. Preventing discrimination by companies
3. Regulating against misleading advertising and 'fine print' contracts
4. Encouraging collective action in the instance of a consumer's rights violation

(ii)

In 2021, various amendments were made to Chile's existing consumer protection law- **Law No.21,398**, with the aim of increasing the scope of consumer protection and strengthening their rights.

(iii)

Cloud Policy

https://www.oecd.org/content/dam/oecd/en/publications/reports/2016/05/digital-government-in-chile_g1g68ee5/9789264258013-en.pdf (i)
https://digital.gob.cl/biblioteca/regulacion/instructivo-presidencial-no1-uso-de-servicios-de-la-nube/ (ii)

The **OECD's Digital Government review** was requested by the Government of Chile in 2016 to help improve the procurement of digital technologies ***only available in Spanish*** in Chile e.g. through the adoption of cloud computing.

The OECD made recommendations on how Chile could align its digital government framework with national ambitions and objectives, moving from an 'e-government' to a 'digital government'. It also stipulated the functions of the Chief Information Officer (**CIO**), responsible for issuing standards and guidelines for priority areas, including cloud computing.

(i)

In 2018, the Digital Government of Chile issued guidelines on the evaluation and adoption of cloud computing services by state administration bodies.

(ii)

Commentary

Data / Privacy

https://digital.gob.cl/biblioteca/regulacion/ley-n-19628-sobre-proteccion-de-la-vida-privada/ (i)

https://www.sernac.cl/portal/617/articles-55451_recurso_7.pdf (ii)

Law No. 19,628 on the protection of privacy was released in 1998 with the aim of regulating the processing of personal data in registries and databases by public bodies/individuals.

(i)

Chile does not currently have a specific supervisory authority in place to enforce regulation pertaining to data protection and privacy. As such, Chile's Consumer Protection Agency (**SERNAC**) are the governing body responsible for protecting data privacy and developing relevant polices and guidelines.

In 2019, SERNCAC issued the **Personal Data Protection Policy.** This sets out to protect consumer's rights in the context of personal data processing, ensuring they have the right to 'informational self-determination'.

(ii)

Fraud

https://www.bcn.cl/leychile/navegar?idNorma=1984 (i)

https://www.bcn.cl/leychile/navegar?idNorma=1195119 (ii)

Chile's laws on fraud are enshrined within the:

1. **Penal Code, 1874.** This covers the various types of fraud; the penalties in place for those who commit fraud; the procedural processes in place when investigating and sentencing. (i)
2. The **Economic Crimes Law, 2023.** This was bought in as an extension of the Penal Code, broadening the definition of fraud and expanding the means of enforcement e.g. increased investigative powers of authorities with the aim to combat white-collar crime and corruption. (ii)

Sanctions

Chile does not have its own independent sanctions list. However, as a UN Member State, they are bound by the **UN Security Council's Consolidated Sanctions lists.**

Terrorism

https://www.oas.org/en/about/who_we_are.asp (i)

https://www.oas.org/oaspage/crisis/crisis_en.htm (ii)

https://www.cmfchile.cl/portal/principal/613/w3-article-55033.html (i)

Chile is a Member State of the Organization of the American States (**OAS**), a group established with the aim of achieving peace and justice across the Americas by promoting solidarity and collaboration.

(i)

Chile is a signatory of the OAS **Inter-American Convention Against Terrorism**. The objective of this Convention is to strengthen co-operation between Member States regarding the implementation of measures to prevent, punish and eliminate terrorism.

(ii)

In accordance with the FATF's 40 recommendations, the CMF made amendments Chile's National Strategy to Prevent and Combat Money Laundering and Terrorist Financing, now placing greater emphasis on **the prevention and detection** of terrorist financing.

(iii)

Commentary

Company Registrar

https://www.registrodeempresasysociedades.cl/ (i)
https://registry.nic.cl/ (i)

In Chile, the company registry is known as the Registro de Entidades Jurídicas (Registry of Legal Entities).It is managed by the Servicio de Registro Civil e Identificación under the Ministry of Justice.

(i)

NIC Chile provides information regarding the Chilean Internet Domain registrations.

(ii)

Access to Public Information

https://digital.gob.cl/biblioteca/regulacion/ley-n-20285-sobre-acceso-a-la-informacion-publica/

Chile's freedom of information (FOI) laws includes the National Constitution's "***probity***" provisions and the Law on Freedom of Opinion and Information and the Practice of Journalism.

Law No. 20,285 on access to public information establishes a system where information is available to all Chilean citizens, regulating the principle of transparency of the public service.

Other

https://www.gob.cl/en/

The official website of the Government of Chile.

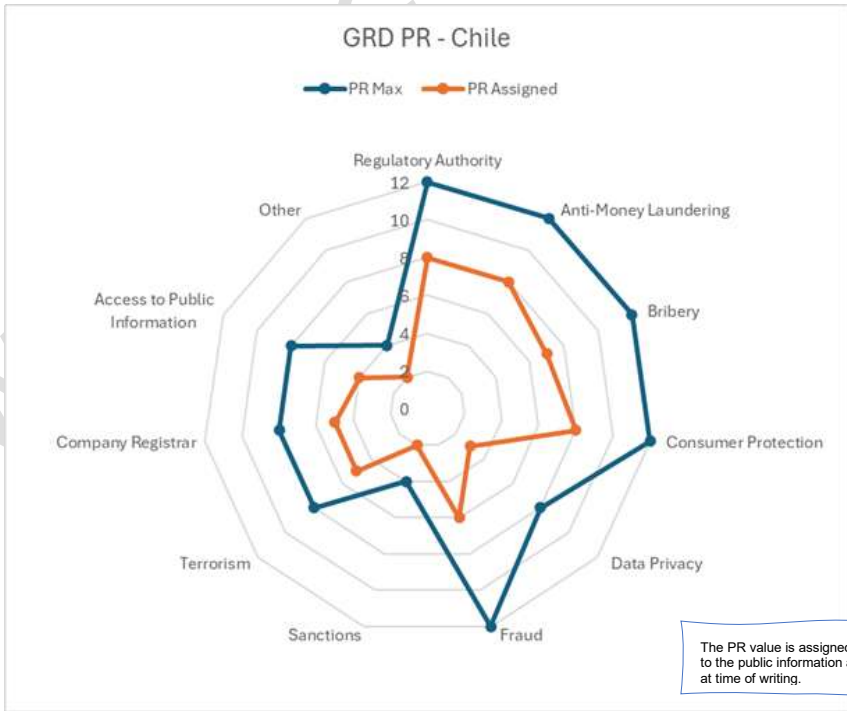
Posture Rating Chile

The PR value of 5.8 is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	8	8	7	8	3	6	2	5	5	4	2

Chile introduced several, regulations and laws which address domain obligations. We observed a lack of digital channels which supported the domains and the lack of clear data privacy processes which impacted the overall scores.

NB: **The figure does not reflect the execution of any processes, laws or regulations**.



Republic of Croatia

Commentary

Financial Regulatory Authority

https://www.hnb.hr/en/home (i)
https://www.hanfa.hr/ (ii)

The Croatian National Bank (**CNB**) is the central bank of the Republic of Croatia. They have been Croatia's national competent authority within the **European Banking Supervision** since 2020.

The main objective of the CNB is to maintain price stability in Croatia. Some of the key functions they perform include:

1. Implementation of monetary policy of the European Union (EU)
2. Foreign exchange operations (transactions) as stipulated in Article 219 of the Treaty on the Functioning of the EU
3. Supervision of credit institutions
4. Regulating and improving payment systems

(i)

The Croatian Financial Services Supervisory Agency (**Hanfa**) is a supervisory authority whose scope include the supervision of financial markets, financial services and legal and natural persons who provide these services. Hanfa is responsible to the Croatian Parliament and has two objectives:

1. Promoting and safeguarding the stability of the financial system
2. Monitoring the legality of the business of the supervisory entities

(ii)

Croatia joined the EU in 2013, however began adopting the **euro** as their official national currency from 2022 onwards.

AI Act / Policy

https://artificialintelligenceact.eu/the-act/ (i)
https://rdd.gov.hr/UserDocsImages/SDURDD-dokumenti/Strategija_Digitalne_Hrvatske_final_v1_EN.pdf (ii)

As an EU Member State, the Republic of Croatia is bound by the **EU AI Act (2024).**

(i)

On a national level, the Government issued the **Digital Croatia Strategy** which aims to increase Croatia's digital and economic competitiveness globally by effectively implementing advanced technologies such as AI in the public and private sector.

(ii)

Commentary

Anti-Money Laundering

https://www.hnb.hr/en/-/legislative-framework (i)
https://www.hnb.hr/documents/20182/123133/e-zakon-pranje-novca-fin-terorizma_npt.pdf/1336f1ec-2e57-a10e-1aae-3dc467fce07c?t=1612435017856 (ii)
https://narodne-novine.nn.hr/clanci/sluzbeni/2011_11_125_2498.html (iii)
https://mfin.gov.hr/highlights-2848/anti-money-laundering-office/2875 (iv)

The two most consequential pieces of legislation in the Republic of Croatia pertaining to the prevention of money laundering (i) are depicted below:

Figure 13 Legislation for Anti-Money Laundering (Croatia)

The Anti-Money Laundering Office (**AMLO**) was established in accordance with the AMLCFT Law as an independent operational unit within the Ministry of Finance.

The AMLO plays a pivotal role in the prevention of ML/TF offences. However, they are not responsible for the investigation of offences. Instead, this power is granted to the relevant prosecution and supervision bodies in the ML/TF system.

(iv)

Bribery

https://narodne-novine.nn.hr/clanci/sluzbeni/2011_11_125_2498.html (i)
https://mpudt.gov.hr/news-25399/croatia-becomes-46th-party-to-oecd-anti-bribery-convention/27657 (ii)

The Republic of Croatia's classification of bribery can be found within the **Criminal Code (2011).** There are several articles covering the different types of bribery offences, including:

1. **Article 294b** - Receiving a bribe in economic or other transactions.
2. **Article 294c** - Offering a bribe in economic or other transactions.
3. **Article 347** - Accepting a bribe.
4. **Article 348** - Offering a bribe.

(i)

Croatia joined the OECD Working Party on Bribery in International Business in October 2023 and became Party to the **OECD Anti-Bribery Convention** in 2024. This involves undergoing peer reviews to monitor and assess the implementation of anti-bribery legislation.

(ii)

Commentary

Consumer Protection

https://www.hnb.hr/documents/20182/2135754/e-zakon-o-zastiti-potrosaca_19-2022.pdf/d73aa75d-d282-107b-9aea-b2ffd4b02d75?t=1654865939985 (i)

https://gov.hr/en/european-consumer-centre-croatia/560 (ii)

https://www.szp.hr/registar-ne-zovi-958/958 (iii)

In 2022, the Government of the Republic of Croatia issued the **Consumer Protection Act.** This regulates the protection of basic consumer's rights when buying products/services, ensuring compliance with various **EU Directives**.

(i)

The **European Consumer Centre Croatia** belongs to the European Consumer Centres Network (**ECC-Net**). They offer advice and information about cross-border purchases and can collaborate with other European Consumer Centres to help consumers resolve disputes/complaints.

(ii)

The **Ministry of Economy and Sustainable Development** are the government department responsible for overseeing matters pertaining to consumer protection. They provide free expert information to Croatian citizens with regards to the protection of their economic interests. Furthermore, they also established a website - the **Central Consumer Portal**, which combines the expertise of stakeholders in consumer protection policy and collates all relevant information regarding consumer's rights in one place.

Consumers can apply to join the public **"Do Not Call"** register if they would like to stop being contacted by traders for the purpose of advertising or selling, without prior consent.

(iv)

Cloud Policy

https://rdd.gov.hr/UserDocsImages/SDURDD-dokumenti/Strategija_Digitalne_Hrvatske_final_v1_EN.pdf

Cloud computing services are an instrumental part of the **Digital Croatia Strategy.** Some of the key pledges in relation to cloud computing are:

1. To increase the usage of the Shared Service Centre (**SCC**), i.e. the 'state cloud', with the aim of integrating the SCC into 300 institutions by 2030.
2. Commitment to continue shaping and improving cloud computing legislation in line with the country's needs and **EU guidelines.**
3. Undergo a digital transformation of education, requiring core investments to e-infrastructure to ensure cloud services and networks can keep up with technological advances.

Commentary

Data / Privacy

https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html (i)
https://azop.hr/national-legislation/ (ii)

The **Act on the Implementation of the General Data Protection Regulation (GDPR)** was issued by the Parliament of Croatia in 2018. As an EU Member State, Croatia is bound by the EU's **GDPR (2016)** and hence, this Act aims to ensure it is implemented in Croatian data protection law.

The Act's scope does not extend to the processing of personal data 'for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

(i)

The **Personal Data Protection Agency**, an independent state body, is responsible for enforcing the Act. They perform various duties, including:

1. Participating in court proceedings in the instance of a GDPR breach
2. Publishing individual decisions on the Agency's website in accordance with the 2018 Act
3. Initiating and conducting procedures against those in breach of the GDPR

(ii)

Fraud

https://narodne-novine.nn.hr/clanci/sluzbeni/2011_11_125_2498.html (i)
https://mfin.gov.hr/glavni-izbornik-2725/highlights-2848/protection-of-financial-interests-of-the-eu/2876 (ii)
https://mfin.gov.hr/UserDocsImages/dokumenti/proracun/Budget%20Act%20-%20consolidated%20text.pdf (iii)
https://mfin.gov.hr/UserDocsImages/en/Protection_EU_financial_interest/minfin_brosura_eng%205_5%20final.pdf (iv)

The various types of fraud are covered within the Croatian **Criminal Code** include:

- Article 121 - **Electoral** Fraud
- Article 224 - **General** Fraud
- Article 224a- **Computer** Fraud
- Article 344 - Fraud in the Performance of a **Duty** (i)

The protection of financial interests of the EU is guaranteed through the Anti-Fraud Coordinated System (AFCOS).

(ii)

The AFCOS System is regulated by:

1. The **Budget Act**, which governs budget oversight and all other matters pertaining to public finance management, ensuring appropriate measures are implemented to prevent financial irregularities and fraud. (iii)
2. Croatia's **regulatory framework protecting the EU's financial interests.** This outlines the functions of the AFCOS system in Croatia and the measures taken so far to report and combat fraud and irregularities.

(iv)

Commentary

Sanctions

https://mvep.gov.hr/foreign-policy/restrictive-measures/271988

As an EU Member State, Croatia adopts sanctions and restrictive measures in accordance with the EU's Security Council Resolutions.

Terrorism

https://www.hnb.hr/documents/20182/123133/e-zakon-pranje-novca-fin-terorizma_npt.pdf/1336f1ec-2e57-a10e-1aae-3dc467fce07c?t=1612435017856 (i)

https://www.soa.hr/en/areas-of-activity/terrorism/ (ii)

The Anti Money Laundering and Terrorist Financing Law (**AMLCFT**), 2017 (most recently amended in 2022), aligns Croatian legislation with the EU Acquis Communautaire. It stipulates the measures, actions and procedures that obliged entities must take to prevent and detect terrorist financing occurring within Croatia's financial system. (i)

The Republic of Croatia's Security and Intelligence Agency (**SOA**) is the governing body responsible for the prevention and combatting of terrorism in Croatia. (ii)

Company Registrar

http://www1.biznet.hr/HgkWeb/do/language?lang=en_GB (i)

https://sudreg.pravosudje.hr/registar/f?p=150:1:0::NO (ii)

The Croatian Chamber of Economy's Company Directory is a comprehensive database that includes all registered business entities in the Republic of Croatia. (i)

The court business register is maintained by the Croatian Ministarstvo Pravosuda Republike Hrvatske (Ministry of Justice). Registered corporations have a court-assigned company matični broj poslovnog subjekta – **MBS** (registration number). The site allows one to searched by MBS or legal name. Search results provide MBS and OIB numbers, registration court, company name, status and address. At time of writing there was no English User Interface. (ii)

Access to Public Information

https://vlada.gov.hr/access-to-information/15017 (i)

https://narodne-novine.nn.hr/clanci/sluzbeni/2013_02_25_403.html (ii)

In 2013, the **Law on the Right to Access Information** was enacted by the Government of the Republic of Croatia. The purpose of the Act is to guarantee the right of access to information and the re-use of information by legal and physical persons. (i)

One of the key features of the Act is the designation of an **Information Officer**, responsible for the following:

1. Regularly publishing information and handling individual requests to access and re-use information
2. Improving the processing, classifying, storing and publishing of information
3. Aiding applicants with regards to exercising their rights in accordance with the law

(ii)

Other

https://vlada.gov.hr/en

The official website of the Government.

Posture Rating Croatia

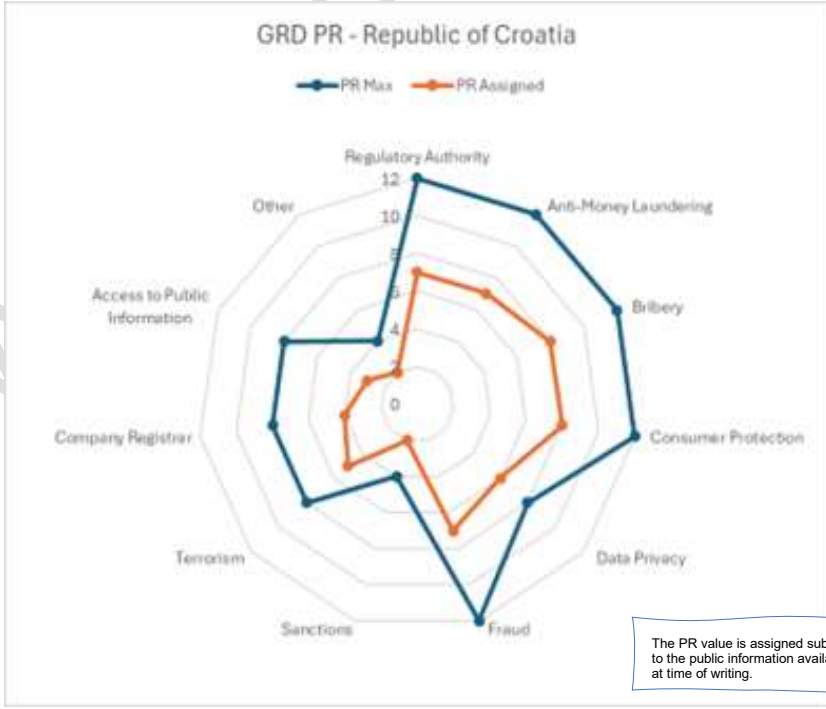
The PR value of **5.9** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	7	7	8	8	6	7	2	5	4	3	2

The Republic of Croatia has several defined processes, regulations and laws to address its domain obligations. However, we observed several weaknesses in the digital channels that support the domains and a weakness in the general access to public information.

Documents were available in the official language and in some cases no translations were available on the public websites.

NB: **The figure does not reflect the execution of any processes, laws or regulations**.



Cyprus

Commentary

Financial Regulatory Authority

https://www.centralbank.cy/ (i)

https://www.gov.cy/mof/en/ (ii)

The main financial regulatory authority in Cyprus is the Central Bank of Cyprus (**CBC**), established shortly after gaining its independence in 1963. Today, the CBC is governed by the now amended Central Bank of Cyprus Law, 2002.

The key objective of the CBC is depicted below:

Figure 14 Core Objectives of the Central Bank of Cyprus (CBC)

After joining the euro area in 2008, the European Central Bank (**ECB**) is now responsible for setting the interest rates of the CBC. Their primary objective is to achieve price stability i.e. keeping interest rates below, but close to, 2%.

The CBC is comprised of 8 Board of Directors: 1 Governor, 2 Executive Members and 5 Non-Executive Members.

1. Supervising the Banks
2. Collecting, compiling and distributing statistical data
3. Promoting, regulating and overseeing the smooth operation of payment and settlement systems
4. Implementing the European Central Bank's monetary policy decisions
5. Holding and managing the official international reserves
6. Safeguarding the stability of the financial system

(i)

The Cypriot Securities and Exchange Commission under the Ministry of Finance.

(ii)

The national currency of Cyprus is the **euro**.

Commentary

AI Act / Policy

https://www.gov.cy/dmrid/en/documents/national-strategy-for-artificial-intelligence/ ***document not available online in English***.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689

The National AI strategy in Cyprus is based on the four main pillars of the European Commission (EU) coordinated plan, "*Artificial Intelligence with the stamp of Europe*". These pillars are as follows:

1. Maximising investments through partnerships.
2. Creation of national data spaces.
3. Cultivating talents, skills and lifelong learning.
4. Developing ethical and reliable AI.

(i)

As an EU member state, Cyprus must comply with the European Parliaments' AI act, 2024. The purpose of this regulation is to provide a uniform legal framework, promoting the uptake of human centric and trustworthy AI i.e. serving as a tool for people, with the aim of increasing human well-being, whilst protecting fundamental rights, democracy, the rule of law and environmental sustainability.

The European Parliament's Artificial Intelligence (AI) Act is a regulation that came into force on August 1, 2024.The Act imposes several regulations on the use of AI in EU member states. These are as follows:

1. A ban on certain AI applications that threaten citizens' rights e.g. AI that manipulates human behaviour/exploits people's vulnerabilities
2. Use of biometric identification systems (RBI) by law enforcement bar a few exceptions e.g. targeted search for a missing person or preventing a terrorist attack
3. High risk AI systems e.g. within critical infrastructure, must fulfil certain obligations and citizens reserve the right to submit complaints/receive explanations over any system that may affect their right
4. General-purpose AI (GPAI) systems and the models that are based on must meet transparency requirements, including compliance with EU copyright law
5. National regulatory sandboxes and real-world testing made available to SMEs and startups for AI development and testing before market launch

(ii)

Commentary

Anti-Money Laundering

https://www.centralbank.cy/en/licensing-supervision/prevention-and-suppression-of-money-laundering-activities-and-financing-of-terrorism-1

As stated in **The Prevention and Suppression of Money Laundering Activities Laws of 2007** (now recognised as the **AML/CFT Law**), the CBC is responsible for enforcing legislation relating to financial activities such as credit, payment, electronic money, currency exchange, leasing and credit acquiring institutions.

The CBC collects prudential returns and reports from entities under their supervision within a specified timeframe and reference period. These are then channelled into off-site monitoring programmes which dictate the appropriate action programmes, including on-site inspections.

Law 58(I) of 2016 states that the CBC is responsible for the compliance of entities under their supervision with targeted financial sanctions, decided and imposed by the United Nations' Security Council and the EU. The CBC also works closely with the Ministry of Foreign Affairs and Ministry of Finance, transferring information regarding lists of countries and/or persons whereby sanctions have been imposed.

Bribery

http://www.cylaw.org/nomoi/arith/CAP161.pdf

Cyprus has a strong anti-corruption framework and consequentially enforces stringent laws against bribery, or any other transactions deemed to be corrupt e.g. fines, imprisonment or a combination of the two.

Chapter 161 of 'The Laws', Cyprus- Prevention of Corruption, states that any person who intentionally accepts, obtains or agrees to accept gifts/rewards in return for doing (or forbearing to do) an action which compromises his or her official duties will be deemed guilty of an offence and liable to a criminal conviction.

Consumer Protection

https://consumer.gov.cy/gr/ (i)
https://consumer.gov.cy/assets/modules/wnp/articles/202302/95/docs/nomos_112-2021.pdf (ii)

The authority responsible for consumer policy in Cyprus is the **Ministry of Energy, Commerce and Industry (MECI)**. The **Consumer Protection Service** is specifically responsible for enforcing legislation relating to protecting consumers in the fast-paced and highly competitive markets of today. Some of the areas covered by their jurisdiction include:

1. Consumer rights
2. Unfair commercial practises e.g. misleading and comparative advertising
3. Conditions for the sale of goods at discount prices
4. Indication of product prices
5. Misleading and unfair terms in consumer contracts
6. Product guarantees

(i)

Under the **Consumer Protection Law of 2021 N.112(I)/2021**, passed by the Cyprus Parliament in May 2021, the Consumer Protection Service have now expanded their authority with regards to imposing sanctions, which include administrative fines and the right to apply to court for injunctions in the instance of a violation.

(ii)

Commentary

Cloud Policy

https://dsf.dmrid.gov.cy/2022/05/17/guidance-for-cloud-computing/ (i)
https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/home_el/home_el?opendocument (ii)

The Deputy Ministry of Research, Innovation and Digital Policy are responsible for setting guidance in relation to the use of cloud computing within Cyprus.

Due to Cyprus being an EU member, any cloud-based services that handle personal data must be hosted in Cyprus or in another EU member state. This is to ensure they are fully compliant with General Data Protection Regulation (**GDPR**).

(i)

If there is a strong reason for using cloud providers outside of the EU when handling sensitive data, one must first seek guidance from the Office of the Commissioner for Personal Data Protection, again, to ensure all activities are following GDPR.

(ii)

Data / Privacy

https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/home_el/home_el?opendocument

The Commissioner for personal data protection is an independent public authority responsible for monitoring the implementation of Regulation (EU) 2016/679 (GDPR) and other laws aiming at the protection of individuals with regards to the processing of their personal data.

The Commissioner performs the duties and exercises the powers assigned by the GDPR or any other relevant law in complete independence.

Fraud

https://www.cylaw.org/nomoi/arith/CAP148.pdf

Cyprus has several laws which address fraud, including laws that cover ;fraudulent transactions, cybercrime and asset tracing. Under section 36 of the Cypriot **Civil Wrongs Law** (Cap.148), fraud is defined as the false representation of fact, made with the knowledge that it is false (or apathetic in determining whether it is true or false), with intent that it shall be acted upon by the person deceived.

As stated in the **Directive (EU) 2019/1937 of the European Parliament and of the Council**, Cyprus must comply with Article 325 of the Treaty on the Functioning of the European Union (**TFEU**). This requires Member States to counter fraud and any other illegal activities that pose a threat to the financial interests of the Union.

Sanctions

https://www.cysec.gov.cy/el-GR/Files/AML/94324.aspx/

This URL links to a document was prepared to provide guidance for the regulated entities of the Cyprus Securities and Exchange Commission (CySEC) and to serve as a single source of information on the legal framework of Sanctions and Restrictive Measures.

As a UN member and EU Member State, Cyprus' legal framework with regards to the implementation of sanctions are as follows:

1. Adopting sanctions by the relevant Security Council Resolution in accordance with **Chapter VII of the Charter of the United Nations**, which have direct and immediate application to Cyprus.
2. Following restrictive measures adopted by the Council of the European Union. These are directly enforceable to Cyprus i.e. they do not need to be transposed into national legislation.
3. Comply with any other European legislation or legally binding international instruments in relation to Sanctions and Restrictive Measures.

Law 58(I)/2016 is the piece of legislation that ensures Cyprus' regulated entities are following the UN Sanctions and EU Restrictive Measures. Some key sections within this law include:

- **Section 3(1)** – competent authorities are designated to securing the implantation of Sanctions/Restrictive Measures in Cyprus, pursuant to The Prevention and Suppression of Money Laundering Activities Laws of 2007.
- **Section 4** – strict penalties imposed for non-compliance.
- **Section 6** – transmission of data/information to the Police in the instance that a person is deemed to be in violation of Sanctions and Restrictive Measures.

Terrorism

https://www.centralbank.cy/en/licensing-supervision/prevention-and-suppression-of-money-laundering-activities-and-financing-of-terrorism- (i)

https://www.gov.cy/mjpo/en/public-order-sector/terrorism/#:~:text=The%20National%20Strategy%20for%20the%20fight%20against%20terrorism%2C,and%20the%20response%20to%20a%20possible%20terrorist%20incident. (ii)

The CBC, along with other supervisory authorities are responsible for ensuring obliged entities abide by the provisions of the **Combatting of Terrorism and Victims' Protection Law N. 75(I)/2019.** This includes confiscating property belonging to or controlled by persons engaged in terrorism.

(i)

Cyprus' Council of Ministers approved the National Strategy for the fight against terrorism in October 2014. This focuses on several areas, including:

1. Increased airport security checks
2. Incorporating the EU Directive, permitting the exchange of passenger data **(PNR)**
3. Enhanced traceability of acquisition and possession of weapons
4. Adopting the Anti-Terrorism and Victims Protection Law of 2019
5. Setting up of a Steering Committee for the management of Chemical, Biological, Radiological, Nuclear and Explosive materials **(CBRN-E)**

(ii)

Commentary

Company Registrar

https://efiling.drcor.mcit.gov.cy/DrcorPublic/Default.aspx?cultureInfo=en-AU (i)
https://efiling.drcor.mcit.gov.cy/DrcorPublic/SearchForm.aspx?sc=0&lang=EN (ii)

The Department of Companies and Intellectual Property.

(i)

Service allowing search of the company registrar of Cyprus.

(ii)

Access to Public Information

https://www.cylaw.org/nomoi/enop/ind/2017_1_184/section-sca84cc4e0-146d-4aab-97d7-2cc1ac5781c2.html (i)
https://www.cylaw.org/nomoi/enop/ind/2017_1_184/section-scdab3fa27-dbb4-4745-8c7c-8c5827e86f5c.html (ii)

In accordance with **The Right of Access to Public Sector Information Law of 2017 (184(I)/2017),** any natural or legal person/s has the right to access information held by a public authority, pursuant to the provisions of the law. However, this does not extend to the provision of personal data, regardless of whether the applicant is the subject or a third party. Furthermore, the right does not exist under the following circumstances:

1. The data is regulated under any other specific legislation on access to information
2. It is not in compliance with imposed EU obligations
3. It is punishable as an offence of contempt of court

(i)

Guidance on how to request and access public information. (ii)

Other

https://www.cyprus.gov.cy/portal/portal.nsf/citizen_en?OpenForm
https://www.gov.cy/en/

The official Cypriot Government web portal.

(i)

Government Digital Services portal.

(ii)

Posture Rating Cyprus

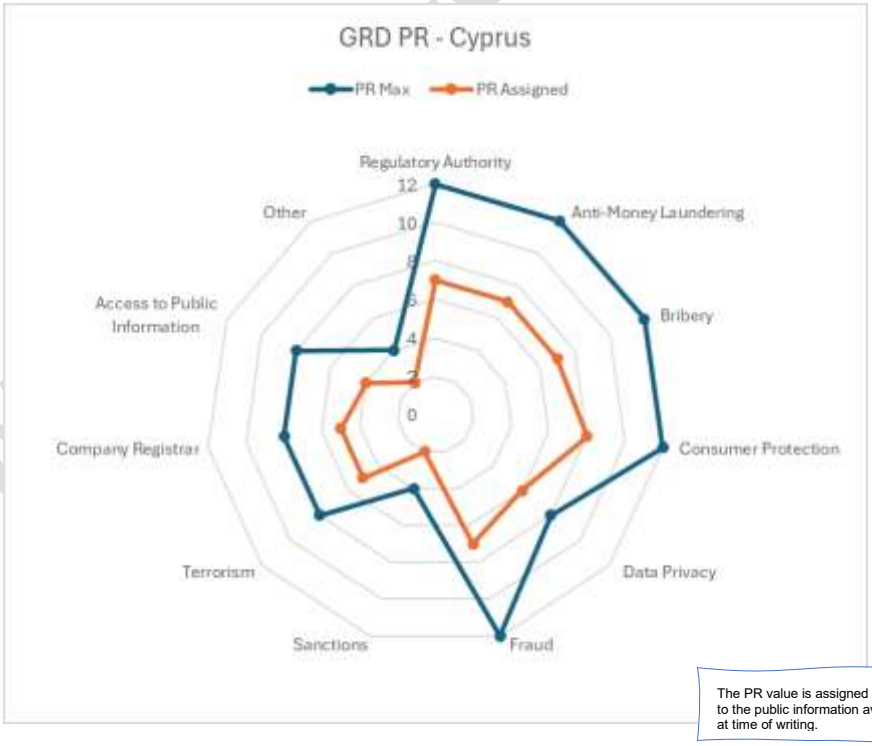
The PR value of **5.9** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	7	7	7	8	6	7	2	5	4	4	2

Cyprus has processes, regulations and laws to address domains and in principle inherits various processes as a member of the European Union.

We observed a lack of maturity in some of the domains and limitations in the digital channels and is reflected in the score.

NB: **The figure does not reflect the execution of any processes, laws or regulations**.



The PR value is assigned subject to the public information available at time of writing.

Czech Republic (Czechia)

Commentary

Financial Regulatory Authority

https://www.cnb.cz/en/ (i)
https://www.cnb.cz/en/monetary-policy/ (ii)

The Czech National Bank (**CNB**) is the central bank and financial market supervisor for the Czech Republic.

The CNB is part of the **European System of Central Banks** and the **European System of Financial Supervision**, contributing to the fulfilment of their tasks and objectives. Some of the main duties carried out by the CNB include:

1. Overseeing the circulation of currency, the payment system and settlement between banks
2. Supervision of financial institutions e.g. the banking sector and the capital market
3. Provides banking services to the state and public sector
4. Conducts transactions in relation to the issuance of government bonds and financial market investments

(i)

The main objective of the CNB is to maintain price stability by keeping inflation as close to the 2% target as possible. It achieves this by adjusting the central bank interest rates in line with market rates and other economic variables e.g. the exchange rate.

(ii)

The official currency of the Czech Republic is the Czech **koruna** and despite being a member of the European Union, has not adopted the euro at the time of writing.

AI Act / Policy

https://artificialintelligenceact.eu/the-act/ (i)
https://www.mpo.gov.cz/assets/en/guidepost/for-the-media/press-releases/2019/5/NAIS_eng_web.pdf (ii)
https://digital-strategy.ec.europa.eu/en/policies/plan-ai#:~:text=The%20Coordinated%20Plan%20on%20Artificial,to%20prevent%20fragmentation%20within%20Europe. (iii)

As an EU Member State, the Czech Republic must comply with the **EU AI Act (2024).**

(i)

In 2019, the Ministry of Industry and Trade issued the **National AI Strategy of the Czech Republic** as part of their 2019-2030 Innovation Strategy.

The strategy sets out a series of objectives and tools to bolster AI development within academia, as well as the public and private sectors, with the aim of making the Czech Republic an innovation leader.

On a European level, the strategy aims to align the Czech Republic with the initiatives of the European Commission (EC) the **'Coordinated Plan on Artificial Intelligence (2018)'**.

(ii)

The EC's Coordinated Plan on Artificial Intelligence is a 'joint commitment between the Commission, EU Member States, Norway and Switzerland to maximise Europe's potential to compete globally'.

(iii)

Commentary

Anti-Money Laundering

https://www.mfcr.cz/assets/attachments/Narodni-strategie-na-ochranu-financnich-zajmu-EUpro-programove-obdobi-2014-2020-anglicka-verze.pdf (ii)

https://www.cnb.cz/en/supervision-financial-market/legislation/money-laundering/laws-and-regulations/ (iii)

https://fau.gov.cz/en/moneyval-609 (iii)

In 2017, the Ministry of Finance issued the Czech Republic's **National Strategy for the Protection of the European Union's Financial Interests.** As stipulated in this strategy, the Financial Analytical Authority (**FAA**) is the main state body responsible for overseeing ML/TF prevention in the Czech Republic.

The FAA essentially performs the functions of a financial intelligence unit, collecting, analysing and disseminating information on suspicious transactions which are then sent to law enforcement authorities. Additionally, they cooperate with the likes of the CNB and Czech Trade Inspection to supervise compliance with AML/CTF regulations.

(i)

Full list of the Czech Republic's **AML/CFT laws and regulations** can be found on the CNB's website.

(ii)

Whilst the Czech Republic is not a member of the FATF, the country is an active member of **MONEYVAL**- a Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of terrorism ("AML/CFT"). This means that they undergo rigorous monitoring and peer review to ensure they are compliant with international standards, including the FATF's 40 recommendations.

(iii)

Bribery

https://www.oecd.org/en/topics/sub-issues/fighting-foreign-bribery/czechia-country-monitoring.html (i)

https://www.mfcr.cz/assets/attachments/Narodni-strategie-na-ochranu-financnich-zajmu-EUpro-programove-obdobi-2014-2020-anglicka-verze.pdf

(ii)

The Czech Republic is party to the **OECD Convention on Combatting Bribery of Foreign Public Officials in International Business Transactions** and as such, go through rigorous monitoring and peer review by fellow party members to ensure the effective implementation of anti-bribery regulation.

(i)

On a national level, bribery within the Czech Republic is governed by the Criminal Code under the following sections:

Section 331	**Reception** of a bribe
Section 332	**Direct** bribery
Section 333	**Indirect** bribery

(ii)

https://www.mpo.gov.cz/en/consumer-protection/legal-regulations-applicable-to-consumer-protection/act-no--634-1992-coll--on-consumer-protection--243610/ (i)

https://www.mpo.gov.cz/en/consumer-protection/legal-regulations-applicable-to-consumer-protection/act-no--64-1986-coll---on-the-czech-trade-inspection-authority--243605/ (ii)

https://www.mpo.gov.cz/en/consumer-protection/legal-regulations-applicable-to-consumer-protection/act-no--102-2001-coll---on-general-product-safety-and-on-amendment-to-certain-acts--243637/ (iii)

https://www.mpo.gov.cz/en/consumer-protection/consumer-guide/the-consumer-guide--263023/ (iv)

Act No, 634/1999 Coll. on Consumer Protection was issued by the Czech Republic's Consumer Legislation Department. This Act aims to continue incorporating EU rules and regulations in Czech consumer protection law, covering issues such as:

1. The fairness of sales
2. Ban on unfair commercial practices
3. Information obligations and labelling
4. Out-of-court settlements on consumer disputes

(i)

Another key piece of legislation in relation to consumer protection is **Act No. 64/1986 Coll. on the Czech Trade Inspection Authority** (most recently amended in 2020). Some of the key changes as a result of the 2020 amendments were:

1. Clarifying the scope and powers of the Inspection Authority
2. Updates to the law, including, the right of consumers to request information necessary to identify sellers on the internet

(ii)

Pursuant to the law of the European Communities, the Government of the Czech Republic also made amendments to the **General Product Safety Act (No. 102/2001 Coll.)**. The objective of this is Act is to clearly outline the obligations of manufacturers, importers and distributors to ensure products on the market are safe for consumers.

(iii)

The **Ministry of Industry and Trade** is the main state body responsible for overseeing matters pertaining to consumer protection. They also curated the '**Consumer Guide**', which contains a breadth of information regarding consumer's rights, contacts of relevant organizations and details on how to make complaints.

(iv)

Commentary

Cloud Policy

https://nukib.gov.cz/download/publications_en/legislation/Presentation-czech-cloud-regulation%201.pdf (i)

The following are only available in the Czech Language Only;

Additional Useful Links ;

a) https://nukib.gov.cz/images/2021-08-31_vyhlaska-vstupni-kriteria.pdf
b) https://nukib.gov.cz/images/2021-08-31_vyhlaska-bezpecnostni-urovne.pdf
c) https://nukib.gov.cz/download/publikace/legislativa/vyhlaska-bezpecnostni-pravidla.pdf

In 2021, the National Cyber and Information Security Agency (**NUKIB**) issued a **Regulation on the Use of Cloud Computing by Public Authority in the Czech Republic** (i) . This outlines the current regulations in place regarding cloud computing, namely:

1) **Act No. 365/2000** Coll., On Public Authority Information Systems (**ZoISVS**).
2) **Act No. 181/2014** Coll., On Cybersecurity (**ACS**)

In connection with these two items of legislations, NUKIB also issued three decrees on the usage of cloud computing services by public authorities:

a) **Decree No. 316/2021** Coll., on certain requirements for registration in the cloud computing catalogue.
b) **Decree No. 315/2021** Coll., on security levels for the use of cloud computing by public authorities.
c) **Decree No. 190/2023** Coll., on security rules for public authorities using the services of cloud computing providers.

Data / Privacy

https://uoou.gov.cz/media/act-no-110-2019-coll.pdf

only available in unofficial English/German translation (i)

https://uoou.gov.cz/en/about-the-czech-dpa (ii)

The Personal Data Processing Act 2019 (**ZZOU**) was brought in to replace the existing Czech Data Protection Act of 2000.

(i)

The main purpose of the new Act was to integrate the EU legal framework i.e. GDPR, into Czech data protection law.

Considering ZZOU, a new supervisory body, the Czech Data Protection Authority (**DPA**) was introduced to enforce the new law.

(ii)

Commentary

Fraud

https://anti-fraud.ec.europa.eu/investigations/anti-fraud-coordination-service-afcos_en (i)

https://verejnazaloba.cz/en/more-about-public-prosecution/international-cooperation/olaf/ (ii)

https://www.mfcr.cz/assets/attachments/Narodni-strategie-na-ochranu-financnich-zajmu-EUpro-programove-obdobi-2014-2020-anglicka-verze.pdf (iii)

As an EU Member State, the Czech Republic is required to establish an Anti-Fraud Coordinating Structure (**AFCOS**).

(i)

The AFCOS facilitates communication between the main domestic authorities within the Czech Republic and the European Anti-Fraud Office (**OLAF**).

(ii)

As of Sept 2007, the Ministry of Finance of the Czech Republic became the central point of contact for the AFCOS when directly networking with OLAF.

Measures taken by the Czech Republic to combat customs fraud can be found enshrined within the **National Strategy for the Protection of the European Union's Financial Interests.**

Pursuant to EU law, Member States are responsible for preventing, detecting and correcting irregularities and fraud. Therefore, a core focus of the national strategy is to develop a robust anti-fraud system, based on four key strategic pillars:

1. Prevention
2. Detection
3. Investigation
4. Recovery and correction i.e. imposing sanctions.

(iii)

Sanctions

https://fau.gov.cz/en/international-sanctions

The Financial Analytical Office is responsible for the coordination of the implementation of international sanctions in the Czech Republic.

In accordance with Act No 69/2006 Sb. on the implementation of International Sanctions, the Financial Analytical Office (**FAO)** are the supervisory authority responsible for imposing international sanctions in the Czech Republic i.e. the EU's Restrictive Measures.

The Czech Republic are bound by the international sanctions adopted by both the **EU** and the **UN**.

Commentary

Terrorism

https://mzv.gov.cz/jnp/en/foreign_relations/security_policy/countering_terrorism/index.html (i)

https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf (ii)

https://www.mfcr.cz/assets/attachments/Narodni-strategie-na-ochranu-financnich-zajmu-EUpro-programove-obdobi-2014-2020-anglicka-verze.pdf (iii)

The Ministry of Foreign Affairs is the state body responsible for enforcing counter-terrorism regulation in the Czech Republic. The Czech Republic implements its measures in line with the **EU Counter-terrorism Strategy**.

(i)

In 2015, the Government released its **Security Strategy,** with the aim of combatting all forms of terrorism, both on a national and international level.

(ii)

Information regarding the Czech Republic's measures taken to combat terrorist financing can be found enshrined within the **National Strategy for the Protection of the European Union's Financial Interests.**

(iii)

Company Registrar

https://justice.cz/ (i)

https://or.justice.cz/ias/ui/podani (ii)

URL Link for website which provides a capability to search the Czech company registrar.

(i)

URL Link for the website to provision the registration of a Company.

(ii)

Access to Public Information

https://www.mvcr.cz/soubor/act-on-free-access-to-information-1999-pdf.aspx (i)

https://www.czechpoint.cz/public/ (ii)

Act 106/1999 Coll. On Free Access to Information stipulates the rules for the provision of information and the rights of the public to access information.

(i)

Public information can be accessed via the 'Czechpoint' website.

(ii)

Other

https://vlada.gov.cz/en/

Government of the Czech Republic official website.

Posture Rating - Czech Republic

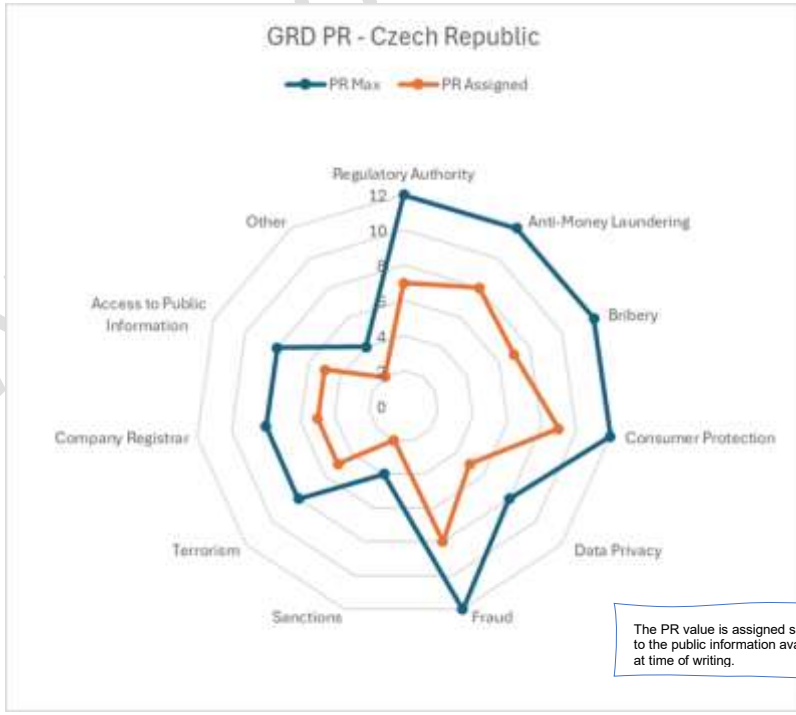
The PR of **6.3** value is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	7	8	7	9	5	8	2	5	5	5	2

The Czech Republic has introduced processes, regulations and laws to address its domain obligations.

We observed weaknesses in the rendering of information via some digital channels. This was offset by the maturity of some of the laws and regulations in place.

NB: **The figure does not reflect the execution of any processes, laws or regulations**.



Denmark

Commentary

Financial Regulatory Authority

https://www.nationalbanken.dk/en (i)
https://www.dfsa.dk/ (ii)

Denmark's National Bank is the Central Bank of Denmark, gaining independence from the country's political system in 1936. The bank has three main objectives:

1. Help to ensure stable prices through a fixed exchange rate policy; keeping the kroner exchange rate stable against the euro
2. Facilitate safe and secure payments through Denmark's online banking service 'Kronos2'
3. Work closely with authorities and the financial sector to help create stability in the financial system

(i)

The Danish Financial Supervisory Authority **(FSA)** also plays a pivotal role in ensuring financial stability in Denmark. Its primary task is to monitor financial undertakings e.g. banks, mortgage-credit institutions, insurance companies etc.and ensure they comply with all relevant obligations.

(ii)

The national currency of Denmark is the Danish **kroner**.

AI Act / Policy

https://en.digst.dk/media/19337/305755_gb_version_final-a.pdf (i)
https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence (ii)

In 2019, the Ministry of Finance with the Ministry of Industry, Business and Financial Affairs published the Danish Government's **National Strategy for Artificial Intelligence.**

The main purpose of the strategy is to provide a roadmap for businesses, researchers and public authorities regarding the responsible development and use of AI, aiding Denmark in becoming a world-leading country in the sector.

The strategy is composed of four key objectives:

1. Ensuring Denmark has a common and ethical human-centred approach to AI
2. Encouraging more research in AI
3. Business growth through AI usage and development
4. Improving public services by exploiting the full potential of AI

(i)

Denmark is an EU Member State. As such, it must also comply with the principles and regulations stipulated in the **EU AI Act of 2024.**

(ii)

Commentary

Anti-Money Laundering

https://www.dfsa.dk/Supervision
https://www.dfsa.dk/Media/638545726607501621/AML_act_2021.pdf

In 2020, the Danish Financial Supervisory Authority (**DFSA**) issued its guide to the act on measures to prevent money laundering and financing of terrorism (the AML Act).

Figure 15. High Level view of the Danish Anti-Money Laundering Act

The guide provides recommendations for individuals on how to meet the requirements stipulated in the AML Act i.e. implementing the **EU's 4th and 5th Anti-Money Laundering Directives**, along with advisories from the Financial Action Task Force **(FATF)** - both of which Denmark are members.

Bribery

https://um.dk/en/-/media/websites/umdk/danish-site/om-os/organisation/antikorruption/anti-corruption-policy-english-version-21072022.ashx (i)
https://home-affairs.ec.europa.eu/policies/internal-security/corruption/eu-legislation-anti-corruption_en (ii)

Denmark's Ministry of Foreign Affairs issued Denmark's **Anti-Corruption Policy** in 2018 ;with the aim a policy of zero tolerance of corruption in all its forms, one of which is bribery.

The policy offers guidance on both foreign and domestic corruption, outlining the appropriate steps to help tackle and prevent it.

The Ministry also curated an **Anti-Corruption Code of Conduct** which explicitly prohibits giving or accepting bribery in any form. (i)

Denmark must also comply with EU legislation relating to combatting corruption. This includes:

1. **The 1997 Convention** on fighting corruption involving officials of the EU or officials of EU countries
2. **The 2003 Council Framework** Decision on combating corruption in the private sector (whereby bribery is criminalised in both an active and passive manner)
3. The 2008 Council Decision **2008/852/JHA**

(ii)

Commentary

Consumer Protection

https://en.kfst.dk/consumer/consumer-regulation/ (i)
https://www.retsinformation.dk/eli/lta/2023/406 (ii)

The regulatory authority responsible for implementing laws in relation to consumer protection in Denmark is the **Danish Competition and Consumer Authority (DCCA).**

Whilst most Danish consumer regulation is enshrined within existing EU regulation, the DCCA will also account for domestic political considerations when drafting new legislation (or making amendments to old ones).

(i)

The most recent regulation issued by the DCCA is the **Law on the right to bring collective actions for the protection of collective interests of consumers, 2023.** The main purpose of this item of legislation is to clearly outline the conditions under which class actions may be taken in the interest of protecting consumer's interests and rights.

(ii)

Cloud Policy

https://en.digst.dk/digital-governance/new-technologies/guide-on-the-use-of-cloud-services/ (i)
https://digst.dk/media/22430/vejledning-i-anvendelse-af-cloudservices-v11-juli-2020.pdf (ii)

In 2020, the **Agency for Digitisation and the Centre for Cyber Security** published guidance for public authorities with regards to the usage and adoption of cloud services.

The main purpose of the document is to ensure authorities are fully aware of the business, legal and information security clarifications required prior to the application of cloud services.

Considering the 2020 ruling made by the EU's Court of Justice, Denmark's guidance on cloud usage was updated, outlining that the **EU-US Privacy Shield** is no longer a valid justification for transferring personal data to the US. As such, a new scheme has been implemented i.e. personal data can now only be transferred to the US from EU Member States if the US organization has been certified by the EU-US Data Privacy Framework.

(i)

Full guide to using cloud services in Denmark available to download on the official **Danish Agency for Digitisation** website.

(ii)

Commentary

Data / Privacy

https://www.datatilsynet.dk/english/about-us/what-we-do (i)
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN (ii)
https://www.datatilsynet.dk/media/7753/danish-data-protection-act.pdf (iii)

The **Danish Data Protection Agency** is an independent national supervisory authority, responsible for upholding the fundamental right of data protection in Denmark.

(i)

There are several pieces of legislation in relation to protecting personal data in Denmark. One of these is **The General Data Protection Regulation (GDPR)**, which all EU Member States are required to comply with (full document can be downloaded from the datatilsynet.dk website).

(ii)

The GDPR is also supplemented by the **Danish Data Protection Act (Act No. 503 of May 2018).** The key elements of this act are as follows:

1. Establish rules on the processing of data i.e. ensuring all processing of data aligns with its original collection purpose
2. Ensuring credit information agencies are informed about data on debts to public authorities
3. Outlining the responsibilities of credit information agencies
4. Stipulating the rights of data subjects
5. Highlighting the powers and duties of independent supervision authorities

(iii)

Fraud

https://um.dk/en/-/media/websites/umen/danida/about-danida/danida-transparency/anti-corruption-policy-english-version-2018.ashx (i)
https://en.fm.dk/media/28633/denmark-s-fiscal-and-structural-plan-2024.pdf (ii)

Denmark's policy on fraud is enshrined within the Ministry of Foreign Affairs 2018 **Anti-Corruption Policy.**

As stipulated in the Anti-Corruption Code of Conduct, fraud is constitutes a criminal offence and defined as any form of "deception, trickery or breach of confidence to gain an unfair or dishonest advantage".

(i)

As part of Denmark's **Fiscal and Structural Policy Plan 2024**, businesses deemed to be at the highest risk of non-compliance or fraud are targeted most frequently for regulatory oversight and ad hoc inspections. The purpose of this is to reduce bureaucracy and ensure an efficient allocation of resources.

(ii)

Sanctions

https://www.nyidanmark.dk/da/Ord-og-begreber/US/Religi%C3%B8se-forkyndere/Den-nationale-sanktionsliste (i)

The Danish Government's official national sanctions list. (i)

Commentary

Terrorism

https://um.dk/en/foreign-policy/terrorism-and-violent-extremism (i)
https://um.dk/en/-/media/websites/umen/danida/partnerships/research/2012/counter-terrorism-and-human-rights.ashx (ii)

Denmark plays an active role in international efforts to combat terrorism. Some of the key policy frameworks that influence Denmark's engagements are as follows:

1. The UN Global Counterterrorism Strategy 2021 (**GCTF**).
2. The EU Foreign Affairs Council Conclusions on EU External Action on Preventing and Countering Terrorism and Violent Extremism 2022
3. The Global Coalition to Defeat ISIL/Daesh
4. The Global Counterterrorism Forum

(i)

Denmark's strategy to counter terrorism is to ensure all national and international obligations are fulfilled, also simultaneously maintaining a human rights/rule of law-based approach.

(ii)

Company Registrar

https://danishbusinessauthority.dk/ (i)
https://datacvr.virk.dk/ (ii)

The Danish Business Authority.

(i)

The Central Business Register providing information for both Denmark and Greenland.

(ii)

Access to Public Information

https://en.digst.dk/digital-governance/data/open-data-and-re-use-of-public-sector-information/ (i)
https://www.datavejviser.dk / (ii)

Considering the **EU Directive on open data and the re-use of public sector information (2019/1024)**, Denmark has updated its landscape of open-data initiatives, promoting the re-use of existing documents and fata collections owned by public authorities.

The primary purpose of this update is to increase the supply of valuable public data, exploiting its full potential for the European economy and society.

(i)

Denmark's Directory for Public Data.

(ii)

Other

https://www.ft.dk/ (i)
https://denmark.dk/ (ii)

The Danish Parliament providing access to various bills.

(i)

Ministry of Foreign Affairs public facing information website.

(ii)

Posture Rating - Denmark

The PR of **6.8** value is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	9	8	8	8	6	8	3	5	6	5	2

Denmark has defined processes, regulations and laws to address its domain obligations. As an EU member state, it has adopted and aligned itself to the relevant regulations which is reflected in the overall score.

NB: **The figure does not reflect the execution of any processes, laws or regulations**.

Egypt

Commentary

Financial Regulatory Authority

https://www.cbe.org.eg/en/ (i)
https://fra.gov.eg/en/ (ii)

The Central Bank of Egypt (**CBE**) is one of the independent regulatory bodies provided for in the Constitution.

The CBE seeks to achieve the sound operation of the monetary and banking system and price stability within the framework of the State's general economic policy, in accordance with the Constitution and the Central Bank and Banking System **Law No. 194** (2020).

(i)

Figure 16. Main duties of the Central Bank of Egypt

The Financial Regulatory Authority (**FRA**) was established in accordance with Presidential Decree **No. 192 of 2009 and Law No. 10 of 2009** and is responsible for monitoring and regulating the non-banking financial sector in Egypt.

Some of the duties that fall under the FRA's jurisdiction are as follows:

1. Establishment and Licensing
2. Regulating and Supervising
3. Inspection and Enforcement
4. Investors and Consumers Protection
5. Financial Awareness and Literacy
6. Developing Non-Banking Financial Markets

(iii)

The national currency in Egypt is the Egyptian **pound**.

Commentary

AI Act / Policy

https://mcit.gov.eg/en (i)
https://ai.gov.eg/SynchedFiles/en/Resources/AIstrategy%20English%2016-1-2025-1.pdf (ii)
https://mcit.gov.eg/en/Me-dia_Center/Press_Room/Press_Releases/66939 (iii)

In 2019, the Egyptian Government established the National Council for Artificial Intelligence (**NCAI**) to expand upon the existing work of the Ministry of Communications and Information technology. The council is comprised of government agencies, academics and leading practitioners in the field of AI. Their main objective is to shape and implement Egypt's National AI Strategy through a co-ordinated approach.

(i)

Egypt's **National Artificial Intelligence Strategy** was first implemented in 2020 and will undergo a phased approach until 2030. The aim of the Strategy is to help strengthen Egypt's regional and global position in the context of AI by creating an AI Industry, including developing *skills, technology, ecosystem, infrastructure and governance mechanisms* to ensure its sustainability and competitiveness.

(ii)

In 2023, the NCAI adopted the **Egyptian Charter for Responsible AI** with the aim of broadening citizens' understanding of Egypt's AI governance frameworks and additionally, ensuring all stakeholders are aware of the ethical considerations required when adopting AI.

(iii)

Anti-Money Laundering

https://mlcu.org.eg/ (i)
https://www.cbe.org.eg/en/aml-cft/egyptian-fiu#atu (ii)
https://www.menafatf.org/about/Members-Observers/members (iii)

The **EMLCU** is an independent unit within the Central Bank of Egypt and responsible for combating money laundering and terrorism financing. The Unit collects and analyses data related to suspicious transactions and works in coordination with law enforcement and other relevant entities.

(i)

The EMLCU was established under the Anti-Money Laundering Law promulgated by Law No. 80 for the year 2002 and it is the Egyptian Financial Intelligence Unit, where the law stipulated in its third article that "An independent Unit".

(ii)

As a member of the Middle East and North Africa Financial Action Task Force (**MENAFATF**), Egypt must also comply with their objectives. This includes incorporating the FATF's 40 Recommendations into AML/CFT regulation.

(iii)

Bribery

https://aca.gov.eg/News/1795.aspx

The Penal Code promulgated by **Law No.58** of 1937 sets out a legal framework for governing against various types of corruption, including bribery which is covered in Chapter 3.

Commentary

Consumer Protection

https://www.cbe.org.eg/en/consumer-protection (i)
https://www.cpa.gov.eg/en-us/About-CPA#:~:text=The%20Consumer%20Protection%20Agency%20of,take%20legal%20actions%20against%20violations. (ii)
http://cpa.gov.eg/Portals/0/Law/CPA-Newlaw.pdf (iii)

The CBE of Egypt recognises consumer protection as one of the most crucial factors in achieving financial inclusion - one of the Bank's key priorities. As such, the CBE issued a set of instructions for banks to follow regarding consumer protection to ensure appropriate protocols were being followed. Additionally, the CBE established the **Consumer Protection Sector**, a group dedicated to promoting trust amongst consumers in the banking sector and ensuring they have full access to financial and legal support when dealing with licensed entities.

(i)

The Consumer Protection Agency (**CPA**) first gained judicial and civil mandates in 2006, pursuant to Egyptian **Law No. 67**. They are supervised by the Ministry of Supply and Internal Trade and serve to protect consumer's rights through various means e.g. monitoring trade activities and ensuring compliance with the Consumer Protection Act.

(ii)

The most consequential piece of legislation in Egypt pertaining to consumer protection is **Law No. 181/2018 on Promulgating Consumer Protection Act.** The law covers the following:

1. General obligations of suppliers and advertisers
2. Specific contract provisions
3. Duties of the CPA
4. Role of NGO's concerned with consumer protection
5. Penalties in place for those in violation of the Act

(iii)

Cloud Policy

https://mcit.gov.eg/en/Publication/Publication_Summary/10525#:~:text=The%20Cloud%20First%20Policy%2C%20align-ing,secure%20and%20sustaina-ble%20digital%20society (i)
https://mcit.gov.eg/Upcont/Documents/Publications_2282024000_Cloud_First_Policy_Egypt_2024.pdf (ii)

In 2024, the Supreme Council of Digital Society adopted Egypt's **Cloud-First Policy**, led by the Minister of Communications and Information Technology.

The strategy was developed in line with Egypt's 'Vision 2030' and 'Digital Egypt' strategies, with the aim of accelerating the use of cloud computing in building a secure and sustainable digital society.

To achieve the vision of the 2024 strategy, Government entities are obliged to commit to adopting a 'cloud-first approach', i.e. prioritising cloud solutions over traditional initiatives. Asides from a list of exempted state bodies, this policy applies to all public and private sector entities.

(i)

A full version of the strategy is available to download from the Egyptian Government's website.

(ii)

Commentary

Data / Privacy

https://mcit.gov.eg/en/Me-dia_Center/Press_Room/Press_Releases/63220

In July 2020, **Law No. 151 on personal data protection** was passed by the president of Egypt, aligning Egypt's data protection legislation more closely with that of the European General Data Protection Regulation (**GDPR**).

The purpose of the law is to protect Egyptian citizens' personal data by providing a comprehensive framework for both data controllers and users, outlining mechanisms for regulating the use of personal data in online advertising and marketing, as well as the digital landscape more broadly.

Fraud

https://fra.gov.eg/en/about-us/ (i)
https://www.cbe.org.eg/en/financial-stability/off-site/fraud-combating-central-department (ii)

The main functions of the FRA involve supervising and regulating non-banking financial markets and instruments in Egypt. This includes taking necessary action to prevent market manipulation and fraudulent activities.

(i)

The Fraud Combatting Central Department (**FCCD**) was established within the CBE to further enhance their role in combating fraud and other financial crimes in Egypt.

The FCCD's main duty is to act as a regulatory and supervisory body for other anti-fraud departments in Egypt, issuing instructions on how to combat fraudulent activities and additionally, monitor the performance and compliance of the CBE's fraud regulations.

(ii)

Sanctions

https://www.cbe.org.eg/-/media/project/cbe/page-content/rich-text/aml-and-cft/laws/antiterrorism-law-organizing-the-lists-of-terrorist-entities-arabic.pdf

Full document on 'Organising the lists of terrorist entities **Law No. 8 for 2015'** can be downloaded from the CBE website.

Terrorism

https://www.cbe.org.eg/-/media/project/cbe/page-content/rich-text/aml-and-cft/laws/anti-terrorism-law.pdf (i)
https://www.fatf-gafi.org/en/countries/global-network/middle-east-and-north-africa-financial-action-task-force--menafa.html (ii)

In 2015, Egypt's Government issued its **Anti-terrorism Law No.94.** Some of the main features of the law are as follows:

- Defining what constitutes terrorism
- Stipulating the powers of security forces when dealing with terror suspects
- Restrictions on freedom of expression if deemed to be inciting terrorism
- Penalties in place for those convicted of terror offences.

- (i)

As a Member State of the **MENAFATF**, Egypt must also endeavour to fulfil the body's objectives when developing polices pertaining to terrorist financing. This includes adopting the FATF's 40 recommendations and implementing relevant UN treaties, agreements and UN Security Council Resolutions.

(ii)

Commentary

Company Registrar

https://www.gafi.gov.eg/English/Pages/default.aspx

An LLC must be registered in the **commercial register** at the General Authority for Investments and Free Zones (GAFI).

An LLC may be 100% owned by foreign investors; however, for an LLC to import goods for the purposes of trading in Egypt, it must be 51% owned by an Egyptian person, entity or company and must have at least one Egyptian manager for importation obligations.

Access to Public Information

https://sschr.gov.eg/en/the-egyptian-constitution/

As stipulated in **Article 68 of the Egyptian Constitution**, all citizens of Egypt have the right to request access to public information.

The Article states that there are specific rules on how the information should be obtained, as well as terms and conditions for its availability and confidentiality.

Other

https://www.presidency.eg/en/ (i)
https://www.sis.gov.eg/?lang=en-GB (ii)
https://www.gafi.gov.eg/English/StartaBusiness/Pages/UsefulLinks.aspx (iii)

The official website of the Presidency - State information Service.

(i)

Government Service Portal.

(ii)

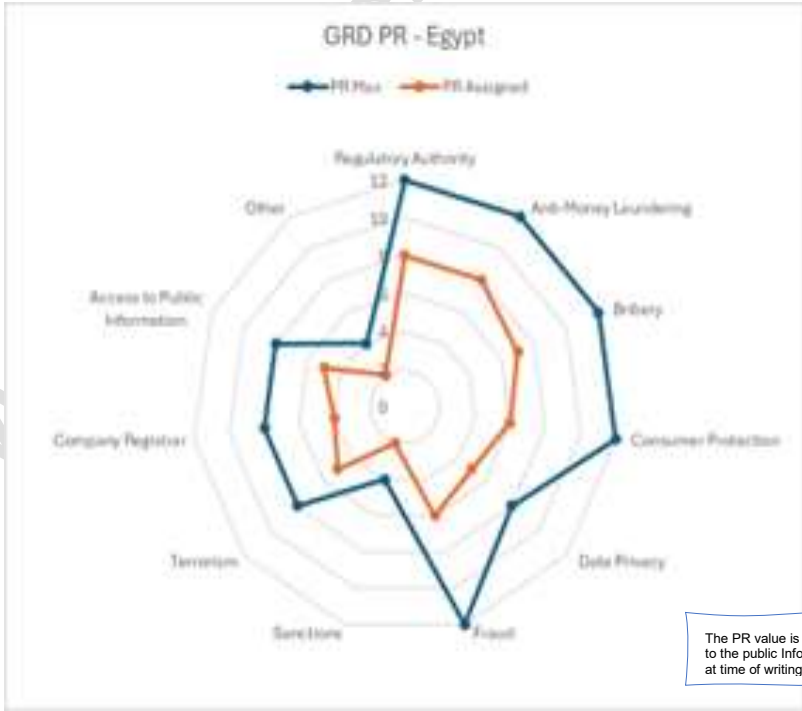
Posture Rating - Egypt

The PR value of **5.8** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	8	8	7	6	5	6	2	5	4	5	2

Egypt has specified processes, regulations and laws to define its domain obligations. Despite the evolution of digital channels in Egypt, we observed some minor weaknesses especially in the domain of consumer protection which is reflected in the assigned value.

NB: **The figure does not reflect the execution of any processes, laws or regulations**.



The PR value is assigned subject to the public Information available at time of writing.

Republic of Estonia

Commentary

Financial Regulatory Authority

https://www.eestipank.ee/en (i)
https://www.eestipank.ee/en/about-us (ii)
http://www.fi.ee/ (iii)

Eesti Pank is the central bank of the Republic of Estonia and a member of the European System of Central Banks.

Eesti Pank manages the **TARGET2-Eesti** settlement system, which is a technical platform for executing monetary policy and is used for fast and secure interbank transfers of funds.

(i)

The main objective of Eesti Pank is to help maintain price stability within the Euro Area. As such, much of Estonia's monetary policy is based around the decisions of the **Governing Council of the European Central Bank.**

Eesti Pank also performs the functions of a traditional central bank, namely;

1. Managing currency circulation
2. Supporting and organising transfers between commercial banks
3. Helping to maintain financial stability within Estonia
4. Managing foreign reserves
5. Preparing key financial statistics and advising the Government of Estonia on economic policy issues

(ii)

The Estonian Financial Supervision Authority.

(iii)

Estonia is a member of the euro system and thus the currency of Estonia is the **euro**.

AI Act / Policy

https://artificialintelligenceact.eu/the-act/ (i)
https://www.kratid.ee/en/kratt-visioon (ii)
https://www.mkm.ee/sites/default/files/documents/2022-04/Digi%C3%BChiskonna%20arengukava_ENG.pdf (iii)

As an EU Member State, Estonia is bound by the **EU AI Act of 2024**.

(i)

Estonia's **National AI Strategy 2022-2023** is for the most part a continuation of the 2019-21 strategy, largely focussing on the adoption of AI solutions in the public and private sector, along with necessary legislative amendments.

The Strategy outlines the Government's plans to increase the use of AI in Estonia and additionally, the measures required to ensure human-centric and trustworthy AI principles are adhered to.

(ii)

Further information regarding Estonia's AI policies is recorded in **Estonia's Digital Agenda up to 2030,** which aims to expand the use of AI in the public sector by engaging in more international and EU-level cooperation through sharing knowledge and expertise on AI solutions.

(iii)

Anti-Money Laundering

https://www.fin.ee/en/financial-policy-and-external-relations/financial-and-entrepreneurship-policy/anti-money-laundering (i)

http://www.fatf-gafi.org/ (ii)

https://www.coe.int/en/web/moneyval/-/moneyval-chairperson-and-fatf-president-exchange-views-with-council-of-europe-committee-of-ministers (iii)

https://www.riigiteataja.ee/en/eli/ee/517112017003/consolide/current (iv)

The Republic of Estonia's Financial Intelligence Unit (**FIU**) is an independent governmental body, under the jurisdiction of the Ministry of Finance. Their mission is to prevent money laundering (ML), terrorist financing (TF) and to perturb financial sanctions within Estonia.

(i)

Estonia is also a member of the Financial Action Task Force (**FATF**) (ii) and the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism. (**MONEYVAL**).

(ii).

Therefore, its AML/CFT laws and regulations are heavily influenced by the associated recommendations and guidelines.

(iii)

The **Money Laundering and Terrorist Financing Prevention Act, 2017** (recently revised in 2024) was implemented to promote trust and transparency in Estonia's business environment, with the aim of preventing the financial system being exploited for the use of ML or TF.

Figure 17 Elements of the Estonian Money Laundering and Terrorist Financing Prevention Act

(iv)

Commentary

Bribery

https://www.riigiteataja.ee/en/eli/515042021003/consolide (i)

https://www.riigiteataja.ee/en/eli/522012015002/consolide (ii)

Article 3 of the **Anti-corruption Act, 2012** stipulates the obligations of public officials and agencies in relation to bribery.

(i)

Estonia's laws on bribery are enshrined within the **Penal Code, 2003** (most recently amended in 2015), under the following sections:

Section 164	Bribery of **electorate**
Section 294	**Accepting** a bribe
Section 296	**Arranging** a bribe
Section 298	**Giving** a bribe
Section 402.3	**Accepting** of a bribe in the **private** sector
Section 402.4	**Giving** a bribe in the **private** sector

Figure 18 Estonia - Penal Code, 2003 Bribery Sections

(ii)

Consumer Protection

https://www.riigiteataja.ee/en/eli/521012014011/consolide (i)

https://ttja.ee/en (ii)

https://ttja.ee/tarbijavaidluste-komisjon (iii)

The **Consumer Protection Act, 2004** (most recently amended in 2014) was issued by the Government of the Republic of Estonia, with the aim of safeguarding consumers rights by regulating the sale of goods or services by traders and establishing the rights of consumers. Additionally, the Act covers the organization and supervision of consumer protection and liability for violations.

(i)

The Consumer Protection and Technical Regulatory Authority (**CPTRA**) was first created in 2019. The main purpose of the Authority is to bolster market and safety regulation in Estonia, ensuring a safer consumer environment for all. Their main functions are as follows:

1. Granting operating rights
2. Advisory services
3. Monitoring various sectors e.g. electronic communications, consumer rights etc.
4. Resolving consumer disputes

(ii)

Within the CPTRA is the **Consumer Disputes Committee**. This is an independent and impartial body, dedicated to settling disputes between consumers and businesses.

(iii)

Commentary

Cloud Policy

https://e-estonia.com/solutions/e-governance/government-cloud/ (i)
https://www.mkm.ee/sites/default/files/documents/2022-04/Digi%C3%BChiskonna%20arengukava_ENG.pdf (ii)

The **Government Cloud** in Estonia was established to promote the modernisation and renewal of existing information systems, enabling the government to harness the full potential of cloud technology.

(i)

Estonia's polices in relation to cloud computing are enshrined within **Estonia's Digital Agenda 2030.** One of the key objectives of the strategy is to ensure Estonia is 'cloud-native'. This includes:

1. Improving digital infrastructure and its ability to implement modern cloud services
2. Increasing the number of specialised cyber security experts in the field of cloud-computing and AI
3. Adopting cloud solutions in the public sector whilst also drawing upon expertise in the private sector

(ii)

Data / Privacy

https://www.eesti.ee/eraisik/en/artikkel/security-and-defense/safety-and-security/protection-of-personal-data-and-privacy (i)
https://www.aki.ee/en (ii)
https://www.riigiteataja.ee/en/eli/523012019001/consolide (iii)

As an EU Member State, Estonia's data protection laws are guided by the General Data Protection Regulation (**GDPR**). This provides the citizens of Estonia the right to request:

1. Information about data being collected on them and its purposes
2. Rectification or deletion of personal data
3. Restricting the processing or transfer of personal data

(i)

The **Data Protection Inspectorate** exists to ensure the citizens of Estonia's personal data is sufficiently protected. They handle and work to resolve some of the following issues:

1. Violation of privacy rights due to the processing of personal data
2. Denied access to personal data in Schengen and Europol databases
3. Spam messages
4. Denied access to Estonian public sector information

(ii)

The Personal Data Protection Act (**PDPA**) of 2018 (most recently amended in 2023) is the most consequential piece of legislation in Estonia regarding data protection and privacy. The Act echoes provisions outlined in the **Regulation (EU) 2016/679 of the European Parliament and of the Council** and additionally, regulates the processing of personal data by law enforcement authorities.

(iii)

Commentary

Fraud

https://www.riigiteataja.ee/en/eli/522012015002/consolide (i)
https://www.fin.ee/sites/default/files/documents/2023-07/Strategy_for_Developing_Financial_Wisdom_in_Estonia_2021%E2%80%932030.pdf (iii)

Estonia's **Penal Code** defines the various types of fraud and penalties in place for those convicted under the following sections:

- **Section 165** - Election fraud
- **Sections 209-213** - General fraud i.e. offences against all types of property
- **Section 316** - Fraudulent creation of evidence
- **Section 349** - Fraudulent use of identity documents
- **Division 4** - Tax fraud

(i)

Estonia's policies in relation to tackling financial fraud are enshrined within the **'Money Smart Estonia' Strategy for 2021-2030.** This includes increasing consumer awareness of financial fraud and ensuring that available support is sufficiently signposted.

(ii)

Sanctions

https://www.vm.ee/en/activity/international-sanctions/sanctions-government-republic-estonia

In 2020, the Republic of Estonia issued the **International Sanctions Act** (most recently amended in 2024). This Act regulates:

1. The implementation of international sanctions in Estonia
2. Specifications for implementation and application of financial sanctions
3. Procedures for monitoring and reviewing sanctions in Estonia
4. Liability in the instance of a violation

Terrorism

https://kapo.ee/en/content/general-information-0/ (i)
https://www.riigiteataja.ee/en/eli/522012015002/consolide (ii)
https://www.riigiteataja.ee/en/eli/ee/517112017003/consolide/current (iii)

The Estonian Internal Security Service (**KAPO**) is the leading authority in Estonia responsible for maintaining national security and fighting against terrorism. They do this by employing various preventative measures in line with state law, including collecting and processing information for the purposes of preventing and combatting terrorism.

(i)

Estonia's Penal Code outlines the various types of terror-related offences under sections **237-237.3.**

(ii)

The **Money Laundering and Terrorist Financing Prevention Act** is another significant piece of legislation with regards to deterring and combatting the financing of terrorism in Estonia.

(iii)

Commentary

Company Registrar

https://www.rik.ee/et/euroopa-ariregister (i)
https://ariregister.rik.ee/eng (ii)

E-services of national register and information system.

(i)

The e-Business Register.

(ii)

Access to Public Information

https://www.riigiteataja.ee/en/eli/ee/503052023003/consolide/current (i)
https://avaandmed.eesti.ee/ (ii)

The **Public Information Act, 2023** ensures that the citizens of Estonia have the right to access information intended for public use. This also covers the re-use of public information.

(i)

Data in the public sector with unrestricted access along with licensed data shared by the private or third sector can be accessed via Estonia's **open data portal**.

(ii)

Other

https://valitsus.ee/en

The Republic of Estonia's official government website.

Posture Rating - Estonia

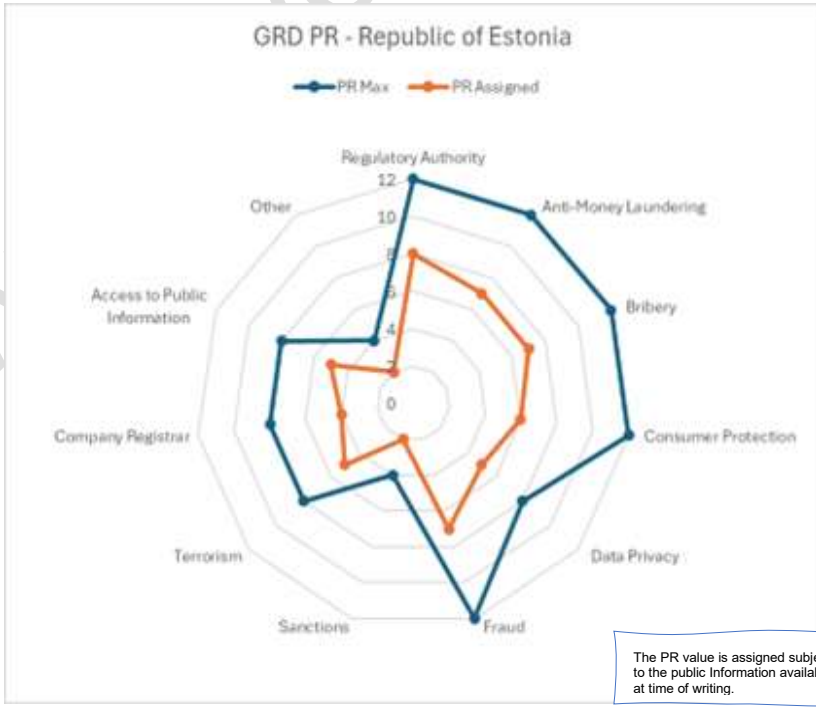
The PR value of **5.8** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	8	7	7	6	5	7	2	5	4	5	2

The Republic of Estonia has aligned its processes, regulations and laws with the EU which are subsequently documented at the various government websites.

We observed some weaknesses in the digital channels, an example being that sanctions information whilst available, lacks clear identifiers e.g. passport numbers which is reflected in the assigned value.

NB: **The figure does not reflect the execution of any processes**



France

Commentary

Financial Regulatory Authority

https://www.banque-france.fr/en (i)
https://www.amf-france.org/fr (ii)

The **Banque de France** is an independent institution of the French Republic and is a member of the Eurosystem;

Its mission can be identified through three key agendas:

1. **Monetary Strategy** – to use the insights and the analysis gathered by key decision makers and economists to ensure price stability and the smooth financing of the economy; as well as operating the implementation of euro area monetary policy. A key tenet of its philosophy is ensuring confidence in the euro
2. **Financial Stability** – to ensure balanced growth within the financial system through supervision over payment systems infrastructure as well as monitoring the activities of financial agents to mitigate potential risk and provide an analysis of future market trends and their impact on economic growth
3. **Services** to the economy and the society – The Banque de France facilitates the accessibility of the public to banking services, maintains Treasury accounts and aims to promote financial and budgetary literacy

The Banque de France has two main representative offices outside of Paris i.e. New York and Singapore and have posted representatives across the globe in various sites.

(i)

The Autorité des Marchés Financiers (**AMF**) regulates the French financial marketplace, its participants and the investment products distributed via the markets. As an independent public authority, it has regulatory powers and a substantial level of financial and managerial independence.

(ii)

France is a member of the Euro system and thus the currency of France is the **euro**.

Commentary

AI Act / Policy

https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence (i)

https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law (ii)

Being a Member of the European Union, France is bound by the EU AI Act which applies from August 2024.

(i)

The use of Artificial Intelligence and the need for a necessary protocol to mitigate any potential risk to businesses and individuals alike has been discussed as part of the EU's Digital Strategy; with the initial regulatory framework for AI being produced by the European Commission in April 2021.

Through defining the type of risk for instance '*unacceptable risk*' and *'high risk'* within its adopted regulatory framework, AI and its potential benefits and threats can be clearly outlined.

The generic framework which France follows is closely aligned to the European Directives and Legislation relating to novel technologies, AI and products contained therein.

Through the agreed negotiations with member states discussions have centred on AI regulation and the issue of safety and compliance, with the measures to adopt AI focussing heavily on this.

(ii)

Anti-Money Laundering

https://www.fatf-gafi.org/en/countries/detail/France.html#:~:text=Member%20since%201990&text=France%20is%20achieving%20particularly%20good,high%2Dend%20money%20laundering%20cases. (i)

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L0849 (ii)

https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006072026 (iii)

France is a member the 'Financial Action Task Force' (FATF) and has been a member since 1990. The country has been particularly effective in complying with the 2022 FATF recommendations, with its mutual evaluation report ensuring a high degree of response to the suggestions relating to compliance and money laundering. The country achieved a particularly good result in the use of financial intelligence, with a high number of high-level prosecutions relating to money laundering cases and offences.

(i)

On a European Level, in relation to AML requirements, France is duty bound in recognition of the fact that it is a member of the European Parliament, to follow more generally and subject to amendment Directive (EU) 2015/849 as well as Directive (EU) 2018/842 relating to anti-money laundering within the financial system and terror financing.

(ii)

Finally, on a national level, The Monetary and Financial Code is followed as well as the AMF General Regulation.

(iii)

Commentary

Bribery

https://www.agence-francaise-anticorruption.gouv.fr/en/lagence (i)

As an integral part of its anti-corruption agenda, the French government has devised a set of protocols enshrined in legislation to combat issues such as bribery, influence-peddling and the taking of undue influence, extortion relating to those in a public office as well as a host of other issues. The information relating to the country's rules and regulations relating to anti-corruption measures can be found on the 'Agence Français Anticorruption'.

On the Website, the public is told that the AFA or the '**French Anticorruption Agency'** was created by the T**ransparency, Anti-Corruption and Economic Modernisation Act 2016-1691** (or the 'Sapin 2' Act) which passed on the 9th of December 2016 and oversees anticorruption measures and operations over the entirety of France's territory.

(i)

Consumer Protection

https://commission.europa.eu/system/files/2022-01/national-consumer-organisations-france-december-2021-en.pdf (i)

https://www.service-public.fr/particuliers/vosdroits/N24033?lang=en (ii)

Consumer protection is a fundamental pillar which safeguards the economic activities of consumers and vendors alike, in France the corresponding link denotes the bodies and policies relating to consumer protection and disputes – which can be found through the European Commission's website.

(i)

Further guidance can also be found on the official website of the French Administration, in the information relating to consumer protection.

The website link makes clear the fact that information on prices and sales is regulated. The website also denotes the duties and obligations to protect the consumer after the acquisition of a good if it is deemed to be defective or problematic as well as other information on mediators and councillors who can offer advice on these issues.

Within the Information and Consumer Section, there are further links relating to;

1. Price
2. Scales, promotion of reduction, liquidation
3. Doorstep sales
4. Mandatory quotations and their affected activities
5. Sales and Purchase Agreements
6. Delivery of goods bought by an individual from a professional
7. Time limitations on reflection and withdrawal
8. Disputes

(ii)

Commentary

Cloud Policy

https://presse.economie.gouv.fr/promulgation-de-la-loi-visant-a-securiser-et-reguler-lespace-numerique-sren/

Regulation of the digital landscape, protection of France's digital sovereignty and easing the transition towards a more digitised society has been at the forefront of the agenda in terms of technology policy.

The most fundamental aspect of this agenda has been marked by the **SREN law**, this law focusses on the following tenets;

1. To protect citizens and minors from the emergence of online threats
2. The establishment of a network of regulators for monitoring purposes
3. The establishment of a digital citizen reserve

However, one of the most fundamental transitions brought on by the SREN Law. This has led to the acceleration of the Cloud transition of the French Economy.

This is rooted in a desire to reduce dependency on and the monopolising influences of cloud computing provider companies. The hope is to achieve this by preventing and reducing lock-in practices of digital tech giants as well as overcoming the practices which lead to the distortion of competition. The aim is to create a more inclusive and fairer tech market.

The administration of the SREN Law is under the supervision of the Digital Services Regulations(**DSA)** and Digital Market Regulations (**DMA**) bodies.

It is important to note that Article 7 of the SREN Bill focusses on the regulation of Cloud credits, which serves to limit the timing conditions and exclusivity provisions of these offerings – this corresponds with limiting the undercutting of competition and creating a fairer arrangement across the digital space.

The SREN law in its entirety should be compatible with the EU's Data Act.

Data Privacy

https://www.cnil.fr/fr/professionnel

The French Data Protection Authority (*Commission Nationale de l'Informatique et des Libertés*) (CNIL) supervises the enforcement of the DPA and frequently issues decisions and guidelines on the DPA.

Fraud

https://www.legifrance.gouv.fr/loda/id/JORFTEXT000037518803

Fraud is generally not considered as a separate criminal offence, but it can form a material element of several criminal provisions, The French Penal Code's **Article 313-1** defines fraud as the act of deceiving someone to obtain money, property, or services.

The French Anti-Fraud Act 2018-898 was adopted on October 23, 2018. The Act was designed to strengthen measures to fight fraud, including; tax evasion, money laundering and social fraud.

Commentary

Sanctions

https://data.europa.eu/data/datasets/consolidated-list-of-persons-groups-and-entities-subject-to-eu-financial-sanctions?locale=en (i)

https://www.tresor.economie.gouv.fr/services-aux-entreprises/sanctions-economiques (ii)

In terms of the sanctions obligations and responsibilities conferred on France by the EU, the French government must comply with acting in compliance with EU guidelines as they relate to financial freezing and compliance regimes involving sanctions within Europe as well as UN Sanctions Directives.

At an international level, information relating to sanctioned individuals, groups and entities can be found on the Europa website, which acts as the official portal for European data and contains consolidated financial sanctions files relating to the entities or individuals involved.

(i)

On the French Treasury website, it outlines that the UN and the Council of the European Union may place financial or trade-restrictive measures on entities, individuals or legal entities. Further, there is a step-by-step process relating to the sanction's measures in force, links to the national freeze register, European Compliance regulations in terms of EU transactions or requests for financial transaction authorization.

(ii)

Company Registrar

https://www.inpi.fr/ (i)

https://www.infogreffe.fr/ (ii)

The Institute National de la Propriété Industrielle (**INPI**) together with Infogreffe, is the central repository of public statutory information on French companies and subsequently supports French business ventures.

(i)

Infogreffe is the **Economic Interest Group** (G.I.E.) bringing together the 141 registries of the commercial courts of France and the overseas departments and regions.

As an extension of the public service mission of the clerks, Infogreffe provides access to legal and economic data on companies registered in the Trade and Companies Register. Thus, individuals have a range of services at their disposal to create and sustain their businesses.

(ii)

Commentary

Terrorism

https://www.amf-france.org/en/news-publications/depth/money-laundering (i)
https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/terrorism-france-s-international-action/ (ii)

France's plan to combat terrorism and its process of curtailing the financing of affiliate organizations and entities is enshrined in its AML-CFT regime. With the EU's Fifth Money Laundering Directive being transferred to French Law at the start of 2020, there was further consolidation of the international stance to adhere to these obligations to confront terror financing.

The Fourth Directive which can be found in the Financial Code of France in 2016 included the obligations contained within this agenda, namely:

1. The conducting of risk assessments
2. Identification and the verification of clients and their beneficial owners
3. Due diligence measures upon entry into business and throughout the course of the relationship
4. The obligation to file suspicious transaction activity reports to TRACFIN.
5. Internal audit and reporting to the AMF
6. Implementation of asset freezing measures

This information is publicly available on the AMF website. (i)

Further information relating to the goals of France's anti-terror campaign can be found on the French government's Diplomacy website; there goals involve but are not limited to;

Figure 19 the French anti-terror campaign high level goals.

France, being a member of the FATF complies with the recommendations of and the inherent obligations to update and expand upon its AML-CTF regime as necessary.

(ii)

Access to Public Information

https://www.service-public.fr/particuliers/vosdroits/F2467

France's Law on Free Access to Administrative Documents (Law No. 78-753 of 17July 1978) was created in 1978 and sets as a rule that citizens can demand a copy of any administrative document (in paper, digitised or other form).

However, Article 6 of the Act provides for a range of exemptions and restrictions which include exemptions in relation to opinions of the Conseil d'Etat (Council of State: combined Supreme Court and Parliamentary Counsel).

The 1978 law came with the creation of the Commission d'Acces aux Documents Administratifs, (**CADA**). The CADA is an independent administrative authority designed to oversee the implementation of the law's provisions and to arbitrate between the public and the administration.

Other

https://www.gouvernement.fr/ (i)
https://www.elysee.fr/en/ (ii)

Official government website. (i)

The official website of the President of France. (ii)

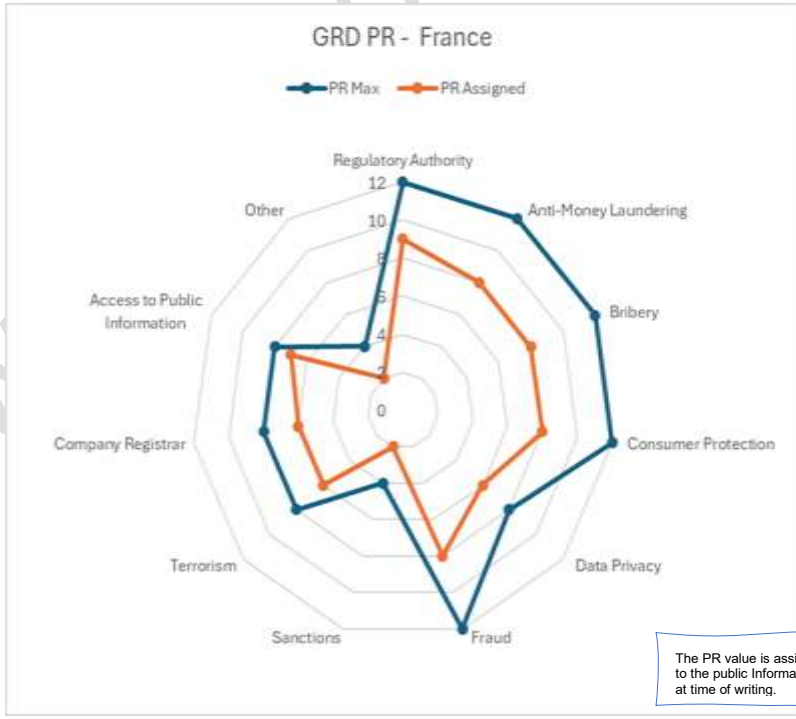
Posture Rating France

The PR value of **7.0** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	9	8	8	8	6	8	2	6	6	7	2

France as a member of the European Union has adopted the processes, regulations and laws to address the domains and has significantly matured these processes within its legislative and other bodies.

NB: **The figure does not reflect the execution of any processes, laws or regulations.**



Finland

Commentary

Financial Regulatory Authority

https://www.suomenpankki.fi/en/bank-of-finland/ (i)
https://www.bankingsupervision.europa.eu/about/thessm/html/index.en.html (iii)

The Central monetary authority in Finland is the **Suomen Pankki** i.e. the Bank of Finland.

Following a referendum, in 1995 Finland became a member of the European Union and is thus a member of the European System of Central Banks.

The Bank of Finland as a member of the Euro System follows central banking guidelines in line with other countries in the Euro Area. In addition to core monetary policy the Bank's central objectives involve financial stability and research into financial statistics as well as banking operations and currency supply.

(i)

The Single Supervisory Mechanism (**SSM**) is the EU Supervisory system with regards to banking and was created by the EU's Banking Union. One of the core objectives of this system is to ensure that the ECB and the national supervisory bodies in member states work closely in cooperation with one another.

The main aims of the SSM are:

- Ensuring the safety and smooth operation of the European Banking System
- The facilitation of further financial integration and stability
- Ensuring consistent supervision of banks

The Finnish authority involved in the SSM is the Financial Supervisory Authority (**FIN-FSA**).

(ii)

Finland adopted the **euro** in 1999.

Commentary

AI Act / Policy

https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/164468/TEM_2022_63.pdf?sequence=1&isAllowed=y (i)

Finland Artificial Intelligence 4.0 Programme focuses on promoting the development and introduction of artificial intelligence and other digital technologies, targeting SMEs in the manufacturing industry.

The AI 4.0 programme is described as promoting the development and introduction of AI and other digital technologies, 'targeting SMEs in the manufacturing sector in particular'. The 'vision' of the AI programme seeks to facilitate a 'twin transition' which alludes to a simultaneous green and digital transformations. The objective is to ensure that Finland's industry will be *'clean, efficient and digital'* by 2030.

It's four key measures regarding development priorities can be seen from the list below:

1. Creating a basis for successful research, development and innovation (**RDI)** clusters through expertise and long-term inputs
2. Enhancing the impact of key technologies through the creation of a national RDI agenda to speed up twin transition
3. Allocating more public funding to products, services and technologies increasing the carbon handprint of digitalisation
4. Ensuring that Finnish Companies are ideally situated to use high performance computing in their business operations

Anti-Money Laundering

https://www.finanssivalvonta.fi/en/financial-market-participants/banks/prevention-of-money-laundering-and-terrorist-financing/current-provisions/ (i)

https://www.finlex.fi/fi/laki/ajantasa/2017/20170444 (ii)

The Finnish Financial Supervisory Authority oversees the country's AML-CFT regimes and policies in place. On the website, there are subsequent lists of the relevant legislation in force governing this type of activity as well as other relevant provisions.

There is reference made to Directive (EU) **2015/849** of the European Parliament and of the Council of 20 May 2015 which relates directly to the prevention of utilization of the financial system for the purpose of money laundering and/or terrorist financing. This was brought into act through amending regulation (EU) No. **648/2012** of the European Parliament.

At a national level, there are also links made to the Finnish Penal Code under the Laws and Regulations Section, referring to Chapter 32 (Money Laundering Offences), Chapter 34a (Terrorist Offences) and Chapter 46 (International Financial Sanctions and Regulations Offences.

(i)

It should be noted that Finland's **Act on the Prevention of Money Laundering and Terrorist** Financing is the main act regarding AML and is supplemented by several separate acts.

(ii)

On the Ministry of Finance Finland's website there is further information relating to the prevention of money laundering and terror financing, including risk assessment frameworks.

Commentary

Bribery

https://oikeusministerio.fi/en/frontpage (i)

https://finlex.fi/en (ii)

Information relating to bribery and other forms of corruption-based crime can be found on Finland's Ministry of Justice website.
(i)
There is also reference on the site to the Finnish Criminal Code which lays down the provisions on bribery offences and the types of bribery offence. The Criminal Code can be found on the Ministry of Justice's database of legislative information FInlexf.fi website.

(ii)

The link to the Criminal code on Finlex.fi is not provided as we found the URL changed frequently but the site does provide the search capabilities.

The types of offences related to bribery also include electoral bribery, (aggravated) giving bribes to a *member of parliament* as well as (aggravated) bribes in *business* context.

It is important that both active and passive bribery are punishable offences and can vary in punishment from a fine to up to two years imprisonment.

Finland's approach to these offences is contained within its anti-corruption agenda.

Consumer Protection

https://finlex.fi/en/legislation/translations/1978/eng/38 (i)

https://www.kkv.fi/en/consumer-affairs/ (ii)

https://www.kkv.fi/en/consumer-affairs/consumer-ombudsman/ (iii)

The Consumer legislation (**38/198**) information can be found on FinLex, the information hub relating to legislation binding both international and national in the country of Finland.

The PDF link outlines the Finnish Consumer Protection Act. Outlined in Chapter One – General Provisions, Section 1 it states that the 'Act applies to the offering, selling and other marketing of consumer goods or services by traders to consumers. The Act generically covers the impact of marketing, consumer rights definitions and the obligations of suppliers.

(i)

The Finish Competition and Consumer Authority is also responsible for dealing with issues relating to consumer affairs, with the website link being outlined as follows. It also enables individuals or entities to report an issue to the Consumer Ombudsman.

(ii)

The Consumer Ombudsman chief purpose it to safeguard the position of 'consumers and supervises compliance with several laws protecting consumer's . It is important to note that the Consumer Ombudsman does not usually deal with individual disputes, with the brunt of these concerns being dealt with by the Consumer Advisory Services and the Consumer Disputes Board.

The Consumer Ombudsman's chief duties in terms of supervision relate to analysing the lawfulness of marketing activities, contractual terms as well as stopping businesses from engaging in unlawful malpractice.

(iii)

Commentary

Data / Privacy

https://tietosuoja.fi/en/legislation (i)
https://www.finlex.fi/ (ii)

The central source for GDPR and data privacy law for Finland would be the website of the Office of the Data Protection Ombudsman.

On the Finlex.fi website the Data Protection Act (**1050/2018**) supplements the EU's General Data Protection Regulation and its national application.

The main goals of the Data Protection Act can be found on the website and are as follows;

1. Supervisory policy and regulations relating to data governance
2. Specification of the age limit for offering information society services to a child
3. Processing of special categories of data
4. Processing of data for journalistic, artistic or academic interest
5. Processing related to personal identity codes
6. Exceptional circumstances in which the public interest could give legal basis for the processing of personal data
7. Restrictions on the rights of the data subject

(i)

A copy of the Act can be found using the search criteria at URL **1050** (Act) and **2018** (year).

(ii)

Cloud Policy

https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165438/VN_2024_7.pdf

Finland's government officially promotes a "cloud-first" approach, encouraging government agencies to utilize cloud services whenever possible as articulated in Finland's National Roadmap.

Finnish government agencies must adhere to EU data protection laws (GDPR) when using cloud services.

Commentary

Fraud

https://poliisi.fi/en/fraud (i)
https://www.kkv.fi/en/consumer-affairs/scams/report-a-scam/ (ii)
https://finlex.fi/en/legislation/collection/1990/769 (iii)

On the Police of Finland's Website, there is a dedicated section denoting the types of fraud people have fallen victim to as well as the activities which are tantamount to or associated with fraudulent conduct. These types of fraud relate to Phishing, Investment Fraud as well as scams on online marketplaces as well as a host of other types of fraud crimes. Guidance and information relating to how fraud victims can contact the police force is also available.

(i)

The Finnish Consumer and Competition Authority also offers information relating to scams relating to false advertising and offers advice on potential remediation measures.

(ii)

In Chapter 36 (**769/1990**) under 'Fraud and Other Dishonesty' of the Finnish Criminal Code the national application of criminal law relating to fraud and conduct associated with fraud is made fully clear.

(iii)

Frauds is defined under Section 1 and suggests that a person who 'obtains unlawful economic benefit' or causes damage to another person' or 'takes advantage of an error of another person' purely for this economic benefit is potentially guilty of fraudulent conduct. There is also information relating to aggravated offences of fraud, petty fraud and insurance fraud.

Sanctions

https://um.fi/international-sanctions (i)
https://www.finanssivalvonta.fi/en/prevention-of-money-laundering-and-terrorist-financing/international-financial-sanctions-and-national-decisions-on-freezing-assets/

Finland is a Member State of the EU and the UN and as such, subscribes to the restrictive measures and sanctions lists imposed by the EU Council and UN Security Council.

The URL link for the Ministry of Foreign Affairs International Sanctions details. It should be noted that some published links at the time of writing were not valid.

(i)

The FIN-FSA International financial sanctions and national decisions on freezing assets is worth visiting to get an appreciation of the Finish Financial Sanctions.

(ii)

Commentary

Terrorism

https://intermin.fi/en/police/counter-terrorism/counter-terrorism-measures-in-finland (i)
https://www.finanssivalvonta.fi/en/prevention-of-money-laundering-and-terrorist-financing/ (ii)

Counter-terrorism measures in Finland are primarily focused on early prevention i.e. identifying the underlying causes that lead to violent radicalisation. There are various authorities in Finland involved in implementing counter-terrorist measures, including:

1. The Police
2. The Finnish Security and Intelligence Service
3. The National Bureau of Investigation
4. The Finnish Border Guard and Finnish Defence Forces and Customs
5. The Finnish Immigration Service
6. The Prison and Probation Service (i)

Preventing the financing of terrorism also plays a crucial role in Finland's anti-terrorism strategy. The Financial Intelligence Unit (**FIU**) is a division within the National Bureau of Investigation- are the main governing body responsible for enforcing legislation pertaining to terrorist financing in Finland.

(ii)

Company Registrar

https://www.prh.fi/en/index.html (i)
https://www.ytj.fi/en/index.html (ii)

Finnish patent and registration office. (i)
The Finnish company registrar search. (ii)

Access to Public Information

https://www.finlex.fi/fi/laki/ajantasa/1999/19990621 (i)
https://oikeusministerio.fi/en/act-on-the-openness-of-government-activities (ii)

The Act on Public Authorities Activities, 1999 (most recently updated in 2023), was issued by the Ministry of Justice to ensure the citizens of Finland have the right to access public information.

The purpose of the Act is to promote transparency and good information practices in Finland, allowing the public to gain an understanding of how public powers and funds are used and further, to provide autonomy over their rights and interests.

(i)

Public information can be accessed through various means. For example, a large amount of information is already available on government ministry websites. Additionally, information that is not publicly available can be requested directly from authorities.

(ii)

Other

https://valtioneuvosto.fi/en/frontpage (i)
https://julkaisut.valtioneuvosto.fi/ (ii)

The Finnish Government Website . (i)

Valto the Institutional Repository for Government which contains publications published in the Ministries' publications series in PDF format starting from the beginning of 2016, some earlier publications and publications by agencies. (ii)

Posture Rating - Finland

The PR value of **6.6** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	9	8	9	7	6	8	2	5	5	4	3

Finland has defined and adopted several processes, regulations and laws to address the domains and international compliance obligations.

Despite the high quality of available information on FinLex.fi we observed weaknesses in the digital channels in relation to some published URLs returning errors and thus failing integrity checks at the time of writing.

NB: **The figure does not reflect the execution of any processes, laws or regulations**.

Federal Republic of Germany

Commentary

Financial Regulatory Authority

https://www.bundesbank.de/en (i)
https://www.bundesbank.de/en/bundesbank/organisation/mission-statement-and-strategy/strategy-2024-618244 (ii)
https://www.bafin.de/EN/DieBaFin/AufgabenGeschichte/aufgabengeschichte_node_en.html (iii)

The Deutsche **Bundesbank** is the central bank of the Federal Republic of Germany.

(i)

Every four years, the Bundesbank's Executive Board come together to develop a long-term strategy for the Bank. The 2024 strategy is founded on four key objectives:

1. Safeguard a culture of stability
2. Enhance the Bank's perceived profile by expanding its services
3. Increase efficiency and ensure the Bank is fit for purpose
4. Strengthen the Bank's role in the Europe i.e. focussing on its role as a partner in the Eurosystem and Single Supervisory System (**SSM**)

(ii)

The Federal Financial Supervisory Authority (**BaFin**) is an independent governing body, subject to legal and technical oversight by the Federal Ministry of Finance. Their main objective is to promote stability and integrity within Germany's financial system.

(iii)

The Deutsche Bundesbank is the German member of the **Eurosystem**. As such, the national currency in Germany is the **euro.**

AI Act / Policy

https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_en (i)
https://www.ki-strategie-deutschland.de / (ii)
https://www.bmwk.de/Redaktion/EN/Artikel/Technology/artificial-intelligence.html (iii)

As an EU Member State, Germany is bound by the **EU AI Act 2024.**

(i)

Germany's national AI policies are outlined in the **Federal Government's Strategy on Artificial Intelligence.** This five-year strategy was first implemented in 2018 and sets out a comprehensive framework for the application of AI in Germany.

(ii)

The primary purpose of the 2018 strategy is to maintain Germany's position as a global AI leader by focussing on 'research, transfer, public dialogue, impact assessment, skills and data availability'.

(iii)

Commentary

Anti-Money Laundering

https://www.bafin.de/DE/Aufsicht/Geldwaeschepraevention/geldwaeschepraevention_node.html (i)

https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Aufsichtsrecht/Gesetz/GwG_en.html (ii)

https://www.zoll.de/DE/FIU/fiu_node.html (iii)

One of BaFin's mandates it to prevent the exploitation of the financial system for the purpose of money laundering, terrorist financing and other financial crimes. To streamline this process further, BaFin established the **Department for the Prevention of Money Laundering** in 2003. They are responsible the supervision of all institutions, companies and specified persons in relation to money laundering.

(i)

The Money Laundering Act, 2018 (**GwG**) is the most significant piece of legislation in Germany pertaining to the prevention of money laundering. BaFin are the regulatory authority responsible for enforcing this law and ensuring the compliance of obliged entities.

One of the primary goals of the GwG is to ensure transparency in business relationships and financial transactions. As such, all supervised entities are obliged to report suspicious transactions to the Financial Intelligence Unit (**FIU**).

(ii)

FIU was established in accordance with **Article 32(1) of Directive (EU) 2015/849**. Information regarding how to report suspicious transactions can be found on their official website.

(iii)

Bribery

https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html (i)

https://www.oecd.org/en/topics/sub-issues/fighting-foreign-bribery/germany-country-monitoring.html (ii)

https://www.bmz.de/resource/blob/23714/1a753885143c47998751f02d702e188c/strategiepapier323-anti-corruption-and-integrity-in-german-development-policy-data.pdf (iii)

The Federal Republic of Germany criminalises bribery in accordance with the **German Criminal Code, 1998** (most recently amended in 2021), under the following sections:

- **Section 108e**- Accepting bribes and/or giving bribes to public officials
- **Section 299**- Accepting and/or giving bribes in commercial practice
- **Sections 299a-300**- Accepting and/or giving bribes in the healthcare sector
- **Sections 331-335**- Accepting and/or giving bribes in public office

(i)

Germany has signed and ratified the **OECD's Anti-bribery Convention.** As such, the country's implementation and enforcement of measures to combat the bribery of foreign public officials is subject to rigorous monitoring and peer-review.

(ii)

Germany's policies in relation to tackling bribery are enshrined within the **Anti-Corruption and Integrity in German Development Policy.** This includes:

1. Tightening legislation and international initiatives to prevent corruption and bribery in the public sector
2. Supporting the implementation of the OECD Convention on Combatting Bribery of Foreign Public Officials

(iii)

Commentary

Consumer Protection

https://www.bundeskartellamt.de/EN/Consumer_protection/Consumer_protection_node.html (i)

https://www.gesetze-im-internet.de/englisch_gwb/ (ii)

The Bundeskartellamt is the leading competition authority in Germany. They play a vital role in protecting consumer rights e.g. by applying German consumer protection laws such as the **Act Against Unfair Competition, 2010** (most recently amended in 2022).

(i)

The Act Against Unfair Competition serves to protect 'competitors, consumers and other market participants against unfair commercial practices.'

(ii)

As a member of the EU, Germany's consumer protection laws must also align with those of the EU Commission.

Cloud Policy

https://www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/digitale-souveraenitaet/deutsche-verwaltungscloud-strategie/deutsche-verwaltungscloud-strategie-node.html (i)

https://www.deutsche-verwaltungscloud.de/ (ii)

The German Administrative Cloud Strategy (**DVS**) was first issued in 2020 by the **IT Planning Council.** The primary aim of the strategy is to standardise Germany's approach to public administration cloud solutions.

(i)

The German government cloud (Deutsche Verwaltungscloud, **DVC**)was launched on 27th March 2025 following an 18-month building phase, offering a secure, standardized cloud services for government agencies everywhere in Germany.

(ii)

Data / Privacy

https://www.gesetze-im-internet.de/englisch_bdsg/ (i)

https://www.bfdi.bund.de/EN/BfDI/UeberUns/DieBehoerde/diebehoerde_node.html (ii)

The Federal Data Protection Act of 2021 is the most consequential piece of legislation in Germany relating to data protection, falling under the jurisdiction of the **Federal Ministry of Interior and Community**.

In addition to its national role in implementing German data protection laws, the Federal Ministry of Interior and Community represents Germany on the European and international stage in shaping general data protection law.

(i)

The **Institution of the Federal Commissioner for Data Protection and Freedom of Information** is an independent supreme federal authority, first introduced in 1978. They also play a crucial role in implementing data protection law in Germany, including the monitoring and enforcement of the EU's General Data Protection Regulation (**GDPR**).

(ii)

Commentary

Fraud

https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html (i)
https://www.bmz.de/resource/blob/23714/1a753885143c47998751f02d702e188c/strategiepapier323-anti-corruption-and-integrity-in-german-development-policy-data.pdf (ii)
https://anti-fraud.ec.europa.eu/policy/policies-prevent-and-deter-fraud_en (iii)

The various types of fraud are stipulated in the **German Criminal Code** under the following sections:

- **Section 107a** – Fraud in connection with elections
- **Section 263** – General Fraud
- **Section 263a** – Computer Fraud
- **Sections 264-265b** – Financial Fraud
- **Section 265c** – Sports betting fraud

(i)

As an EU Member State, Germany's anti-fraud policies are largely driven by the European Commission's Anti-Fraud Office (**OLAF**).

(ii)

The Federal Ministry for Economic Cooperation and Development issued the **Anti-Corruption and Integrity in German Development Policy** in 2012. This outlines Germany's contributions in preventing fraud and corruption on an international level, including, the introduction of a 'Systematic Risk-Based Approach i.e. systematically analysing the risk levels of each country to determine whether additional anti-fraud/corruption measures are required.

(iii)

Sanctions

https://www.bundesbank.de/de/service/finanzsanktionen#tar-1 (i)
https://www.bmwk.de/Redaktion/EN/Artikel/Foreign-Trade/enforcement-of-sanctions-and-sanctions-related-criminal-law/enforcement-of-sanctions-and-sanctions-related-criminal-law.html#doc496bd46b-fd26-4fa3-8d3d-39986dcf4249bodyText1 (ii)

Restrictive measures/sanctions in Germany are determined by:

1. The United Nations Security Council
2. The European Council
3. National authorities

(i)

In May 2022, The Federal Republic of Germany issued the **Sanctions Enforcement Act I.** This served as an initial step towards more effective sanctions enforcement in Germany.

In Dec 2022, the Government then went on to issue **Sanctions Enforcement Act II** which led to a complete structural reform of the enforcement procedure for individual financial sanctions and additionally, stronger of AML measures.

(ii)

Commentary

Terrorism

https://www.nationalesicherheitsstrategie.de/National-Security-Strategy-EN.pdf (i)
https://www.bka.de/EN/OurTasks/SupportOfInvestigationAndPrevention/Research/TerrorismExtremism/researchUnitTerrorismExtremism.html (ii)
https://www.bundesfinanzministerium.de/Content/EN/Standardartikel/Press_Room/Publications/Brochures/2020-07-30-strategy-to-counter-money-laundering.pdf?__blob=publicationFile&v=6 (iii)

In 2023, The Federal Republic of Germany issued its **National Security Strategy**. This highlights the current threats faced in Germany regarding national security (including terrorism) and the intended measures to counteract these threats. For example, increasing international cooperation via Europol and Eurojust to tackle transnational terrorism. (i)

In response to the 9/11 terror attacks of 2001, Germany- along with Spain and the UK- decided that security agencies needed to channel their efforts into understanding the underlying causes of terrorist violence. As such, in 2003, the Extremism Research Unit (**FTE**) was established in Germany. This is a group comprised of both police officers and specialists in the field of social science, working to together with a shared goal of determining the root causes of terrorism/extremism.

(ii)

Another crucial part of Germany's anti-terrorism strategy is to prevent the financing of terrorism. Some of the key measures already in place are outlined in the **Strategy to Counter Money Laundering and Terrorist Financing, 2020.**

The strategy is largely driven by insights from the European Commission's supranational risk assessments (**SNRA**) and Germany's National Risk Assessment (**NRA**). (iii)

Company Registrar

https://www.handelsregister.de/rp_web/welcome.xhtml (i)
https://www.unternehmensregister.de/ureg/ (ii)
https://www.unternehmensregister.de/ureg/search1.2.html;jsessionid=14DDF0ADEDA5EDA69993FFCC32644B68.web01-1 (iii)

The German federal states commercial register, registers of cooperatives, partnerships, civil law partnerships and associations for all German federal states and, additionally, the register announcements (publications) .

(i)

The German central platform for company data.

(ii)

Search capability provided for the company registrar.

(iii)

Access to Public Information

https://www.gesetze-im-internet.de/englisch_ifg/index.html

The Freedom of Information Act, 2006 (most recently amended in 2013) stipulates that every citizen of Germany is entitled to gain access to public information from federal government authorities, providing there are no overriding exemptions/legal provisions.

Other

https://www.bundesregierung.de/breg-en

The official website of the German federal government.

Posture Rating - German

The PR value of **7.0** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	10	8	8	8	6	8	3	6	6	5	2

Germany has well-structured and mature processes, regulations and laws that support the relevant domains.

Germany is also a member of the European Union and as such adopts and promotes many of the rules for the domains.

NB: **The figure does not reflect the execution of any processes, laws or regulations.**

Greece - The Hellenic Republic

Commentary

Financial Regulatory Authority

https://www.bankofgreece.gr/en/homepage (i)
http://www.hcmc.gr/en_US/web/portal/duties (ii)

The **Bank of Greece** is the Central Bank of Greece and as an independent authority, pursues price stability and the stability and smooth operation of the financial system (banks, insurance companies, etc.).

While remaining institutionally and operationally independent, it is subject to democratic control by parliament.

The Bank of Greece is an integral part of the Euro system and, together with the other national central banks of the euro area and the European Central Bank, participates in the formulation of the single monetary policy for the euro area.

(i)

The Hellenic Capital Market Commission (**HCMC**) is a legal entity, established to protect and ensure the smooth operating of the Greek capital market. This includes enforcing capital market legislation and actively participating in the formation of the capital market regulatory framework on a national, European and international level.

(ii)

AI Act / Policy

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689 (i)
http://democratisingai.gr/assets/DEMOCRATISING_AI_final.pdf (ii)

Greece is an EU Member State and as such, must comply with the **EU's AI Act 2024.** - Regulation (EU) **2024/1689.**

(i)

On a domestic level, Greece's AI polices are enshrined within their **National Strategy – Democratising AI.** This strategy is founded on Greece's vision of becoming 'the world's laboratory for Democratising AI in a sustainable way' by effectively integrating AI into society and aligning it with the basic principles of democracy.

(ii)

Anti-Money Laundering

https://www.bankofgreece.gr/en/main-tasks/supervision/prevention-of-money-laundering (i)
https://aml-authority.gov.gr/en/ (ii)

The **Bank of Greece** is the authority responsible for governing the legal and regulatory framework on preventing money laundering and terrorist financing (**AML/CFT**).

Greece's legislative AML/CFT framework is heavily influenced by EU regulation, which also aligns with the Financial Action Task Force's **(FATF) 40 Recommendations**.

(i)

The Authority for Combatting Money Laundering (**HAMLA**) was established, pursuant to Law 4557/2018, to prevent, detect and combat money laundering and terrorist financing, identify suspicious persons and impose necessary sanctions in line with the **UN Security Council Resolutions** and **EU Directives and Regulations**.

(ii)

Commentary

Bribery

https://aead.gr/en/ (i)
https://www.oecd.org/en/topics/sub-issues/fighting-foreign-bribery/greece-country-monitoring.html (ii)

Greece's anti-bribery laws criminalize bribery of public officials, judges and arbitrators. The laws also apply to legal entities that benefit from bribery.

On 15 June 2024, the Council of Ministers unanimously approved the update of the National Anti-Corruption Action Plan 2022-2025 (**NACAP**) available for download.

(i)

Greece is Party to the OECD Convention on Combatting Bribery of Foreign Public Officials in International Business Transactions. As such, they undergo rigorous monitoring and peer-review by the **OECD Working Group on Bribery** to ensure they are successfully implementing anti-bribery measures.

(ii)

Consumer Protection

https://kataggelies.mindev.gov.gr/ (i)
https://www.eccgreece.gr/topics/consumer-goods-and-services/buying-goods-and-services-eu (ii)

The **General Directorate of Market and Consumer Protection** is the governing body responsible for overseeing matters pertaining to consumer protection in Greece.

Information regarding how the various EU Directives and Regulations have been integrated into Greek national laws can be found under 'national legislation' section of their website. (i)

In accordance with EU consumer protection law, Greece has its own European Consumer Centre (**ECC**) and formally participates in the **European ECC Network**.

(ii)

Cloud Policy

https://digitalstrategy.gov.gr/project/g-cloud (i)
https://digitalstrategy.gov.gr/project/g-cloud_next_generation (ii)
https://digitalstrategy.gov.gr/en/vivlos_pdf (iii)

One of the key policies within the **Digital Transformation Bible 2020-2025** is to strengthen the central infrastructures of the Government Cloud (G-Cloud). Some of the actions required for the implementation of this policy include:

1. The completion of two existing government cloud nodes
2. Licencing of existing infrastructure and/or the use of public cloud infrastructure

(i)

Another key project within the strategy is the G-Cloud Next Generation (**NxG**), a set of computing infrastructures created to serve the Public Administration systems. This requires the following measures:

1. Expanding existing computer power and introducing a second data centre
2. Implementing new systems and additionally, updating existing systems so that they follow a 'Cloud Native' infrastructure

(ii)

The full publication of Greece's **Digital Transformation Bible 2020-2025** is available to download from the Government website.

(ii)

Commentary

Data / Privacy

https://www.dpa.gr/en (i)
https://www.dpa.gr/sites/default/files/2020-08/LAW%204624_2019_EN_TRANSLATED%20BY%20THE%20HDPA.PDF (ii)

The **Hellenic Data Protection Authority** is an independent public authority, responsible for supervising the implementation of the EU's General Data Protection Regulation (**GDPR**), national data protection laws and any other regulation in Greece pertaining to the processing of personal data.

(i)

In 2019, the Government of Greece issued the **Data Protection Law, 2019** (**4624/2019**) This law was introduced for the following reasons:

1. To update the existing data protection framework and functions of the Data Protection Authority
2. To adopt new measures for implementing relevant EU Directives and Regulations

(ii)

Fraud

https://aead.gr/images/manuals/esskd/2018-2021/NACAP_2018-2021.pdf (i)
https://aead.gr/en/ (ii)
https://afcos.aead.gr/ (iii)

Greek policies against fraud are enshrined within the **National Anti-Corruption Plan, 2018.** Some of these include:

1. Improving the internal control system and internal auditing- particularly in relation to alleged/detected fraud incidences
2. Increased cooperation across the public sector e.g. when dealing with high level tax fraud
3. Strengthening the role of the Anti-Fraud Coordination Service (**AFCOS**)
4. Developing new fraud-prevention policies e.g. measures to fight fraud in structural funds
5. Introduction of an Anti-Fraud Communications Strategy
6. Standardizing the data collection and reporting of corruption and fraud

(i)

The National Transparency Authority (**NTA**) is an independent authority, responsible for promoting transparency, integrity, control and accountability in Greece. This includes developing policies and practices designed to combat fraud and corruption.

(ii)

The **AFCOS** is a department within the NTA. In 2021, they launched a new online platform with the aim of enhancing the networking capacity of national authorities across the EU, thus moving towards a more coordinated approach in the fight against fraud across the EU Member States.

(iii)

Commentary

Sanctions

https://www.mfa.gr/en/foreign-policy/global-issues/international-sanctions/ (i)
https://www.bankofgreece.gr/en/main-tasks/supervision/sanctions (ii)

The **Financial Sanctions Unit**, a department within the Anti-Money Laundering Authority, is the governing body responsible for implementing the restrictive measures imposed by the **UN Security Council** and **EU Council**. (i)

On a national level, the **Bank of Greece** has the authority to impose administrative penalties on entities under their supervision in the instance of non-compliance with the legal and regulatory framework. Some of the entities under their jurisdiction include:

1. Credit institutions
2. Insurance and reinsurance undertakings
3. Insurance distributors
4. Certain financial institutions e.g. those under liquidation (ii)

Terrorism

https://fsu.aml-authority.gov.gr/en/ (i)
https://www.fatf-gafi.org/en/countries/detail/Greece.html (ii)
https://www.bankofgreece.gr/en/main-tasks/supervision/prevention-of-money-laundering (iii)

One of the main duties carried out by the **Financial Sanction Unit** is identifying persons involved in terrorism or terrorist financing. (i)

Greece has been a member of the Financial Action Task Force since 2019 and hence, aims to incorporate the **FATF's 40 recommendations** into its policies against the financing of terrorism.

(ii)

The **Bank of Greece** is responsible for supervising the compliance of obliged entities with regards to AML/CFT regulation. It is then the duty of the Anti-Money Laundering Authority (**HAMLA**) to conduct investigations into suspicious transactions and implement combative measures where necessary. (iii)

Company Registrar

https://services.businessportal.gr/welcome/ggpsIntro (i)
https://publicity.businessportal.gr/ (i)

URL for registration of a new company in Greece, the **general commercial register**. (i)

The Greek company registrar search from the Hellenic Republic Ministry of Development. (ii)

Access to Public Information

https://data.gov.gr/ (i)
https://repository.data.gov.gr/ (ii)

The full institutional framework governing Greece's 'open data policy' is available on the government website. (i)

Greece's official open data portal. (ii)

Other

https://www.gov.gr/en (i)
https://www.government.gov.gr/ (ii)

The Greek Government's website. (i)

Gov.gr is the new web portal of Greece. It hosts digital service of the ministries, organizations, authorities and regions. (ii)

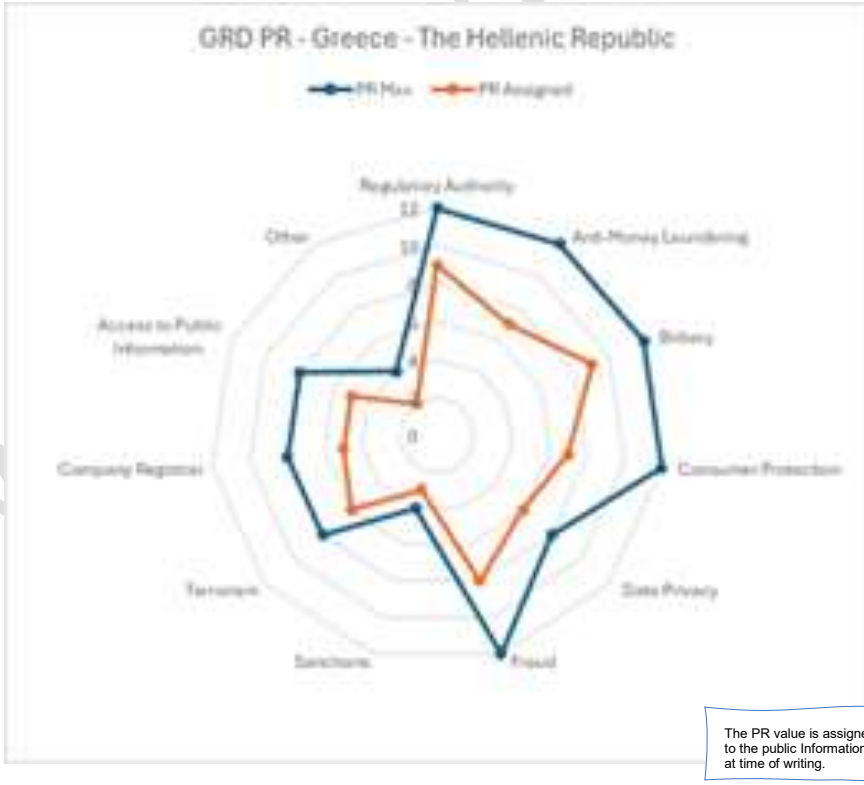
Posture Rating - Greece

The PR value of **6.7** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	9	7	9	7	6	8	3	6	5	5	2

Greece as a member of the EU has adopted processes, supporting regulations and laws that support its domain obligations.

NB: **The figure does not reflect the execution of any processes, laws or regulations**.



The PR value is assigned subject to the public Information available at time of writing.

Hungary

Commentary

Financial Regulatory Authority

https://www.mnb.hu/web/en (i)
https://www.mnb.hu/letoltes/mnb-torveny-2024-09-01-en.pdf (ii)

The **Magyar Nemzeti Bank (MNB)** is the central bank of Hungary. The MNB is a member of the European System of Central Banks. At the website you will find an unofficial translation of MNB Act in English.

(i)

In accordance with **Act CXXXIX of 2013** on the MNB, the Bank and its decision-making bodies function independently from the Government and institutions of the EU whilst carrying out their main duties and obligations. The only body that influences the MNB when performing its duties is the **European Central Bank**.

(ii)

The main objective of the MNB is to achieve and maintain price stability. Additionally, it is also responsible for supporting the Government's economic policies by implementing various monetary policy instruments.

The national currency in Hungary is the **euro**.

AI Act / Policy

https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_en (i)
https://ai-hungary.com/files/api/v1/companies/15/files/146074/download.pdf (ii)

As an EU Member State, Hungary is bound by the **EU AI Act 2024.**

(i)

On a national level, **Hungary's Artificial Intelligence Strategy 2020-2030** outlines various policies and regulations pertaining to AI development and usage in Hungary. The strategy can be decompartmentalised into three key interdependent measures/interventions depicted below:

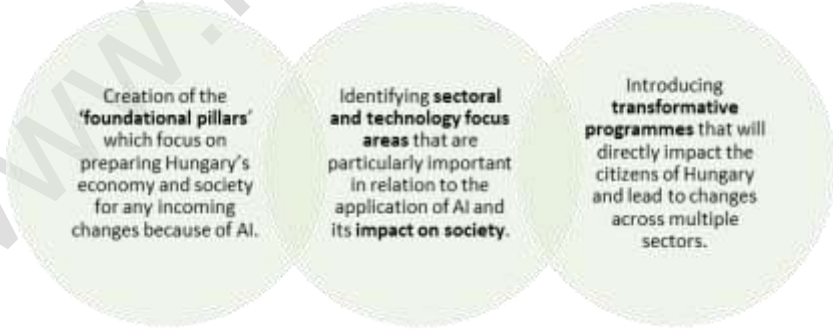


Figure 20 Hungary's interdependent AI measures/interventions

(ii)

Commentary

Anti-Money Laundering

https://www.mnb.hu/letoltes/aml-cft-act-hungary2020.pdf (i)
https://www.fatf-gafi.org/en/countries/detail/Hungary.html (ii)

Act LII of 2017 on Preventing and Combatting Money Laundering and Terrorist Financing is the most consequential piece of legislation in Hungary pertaining to Anti-Money Laundering (**AML**). Some of main areas covered in the Act are as follows:

1. Due Diligence measures
2. Framework for carrying out risk assessments on suspicious entities.
3. Reporting obligations of supervisory authorities and other relevant bodies
4. Duties and powers of the Financial Intelligence Unit (**FIU**)
5. Group level policies and procedures for EU Member States
6. Supervision measures

(i)

As a member of the Financial Action Task Force (**FATF)** and the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (**MONEYVAL)**, Hungary must also seek to incorporate their recommendations into AML/CFT regulations.

(ii)

Bribery

https://thb.kormany.hu/download/a/46/11000/Btk_EN.pdf (i)
https://corruptionprevention.gov.hu/download/c/fe/02000/National%20Anti-Corruption%20Programme%20Hungary%202015-2018.pdf (ii)
https://www.oecd.org/en/topics/sub-issues/fighting-foreign-bribery/hungary-country-monitoring.html (iii)

Hungary's laws on bribery are enshrined within the **Act C of 2012 of the Criminal Code** under the following sections:

- **Section 290-291** - Active *Corporate* Bribery
- **Section 293-294** - Active/Passive Bribery of *Public* Officials (i)

Hungary's domestic policies with regards to combatting bribery are contained within the **National Anti-Corruption Programme Hungary 2015-2018.** One of the main priorities of this strategy is to promote a *clean and transparent business environment* in Hungary. Some of the measures to achieve this objective include:

1. Increasing awareness amongst organizations and institutions within Hungary on international corruption and bribery legislation
2. Implementation of the OECD's Working Group on Bribery's recommendations e.g. Tax Auditors must now receive specific training to detect international bribery

(ii)

Hungary is party to the **OECD Anti-Bribery Convention** and thus, undergoes rigorous monitoring and peer-review in relation to the enforcement of anti-bribery measures.

(iii)

Commentary

Consumer Protection

https://njt.hu/jogszabaly/1997-155-00-00 (i)
https://www.gvh.hu/pfile/file?path=/en/legal_background/rules_for_the_hungarian_market/competition_act/competition-act-documents/jogihatter_tpvt_hataly_20190101_a&inline=true (ii)

The **CLV of 1997 Law on Consumer Protection** is one of the most consequential pieces of legislation in Hungary pertaining to consumer protection. The purpose of the Law is to establish a comprehensive framework for the protection of consumer's interests, particularly in relation to:

1. The safety of goods and services
2. The protection of their financial interests
3. Raising awareness of legal support available and the associations who represent their interests
4. The development of an institutional structure required for enforcing the protection of consumer's interests.

(i)

The Hungarian Competition Authority also shares some responsibility regarding the protection of consumer rights. Provisions in relation to consumer protection are outlined in **Chapter 3 of the Competition Act**, including:

- Prohibition of deceiving consumers in **economic competition**
- Prohibition of unjustified restriction on the freedom of consumer **choice**

(ii)

Cloud Policy

https://www.dmu.gov.hu/ (i)
https://www.dmu.gov.hu/documents/prod/Nemzeti-Strategiai-Utemterv_vegl.pdf (ii)

The Digital Hungary Agency (**DMÜ**) is responsible for supervising the Hungarian government's IT systems and infrastructure, as well as the implementation of e-public administration. One of the key priorities of the DMÜ is to create a **Hungarian-based cloud service**.

(i)

Hungary's **National Strategic Agenda for achieving the Digital Decade** Policy Programme 2030 outlines various measures planned to promote digital development and strengthen Hungary's digital economy. Some of these include:

1. Increase Hungary's competitiveness through the implementation of modern cloud technology
2. Support and promote a wide-scale introduction of cloud-based solutions in public services

(ii)

Commentary

Data / Privacy

https://www.naih.hu/about-the-authority (i)
https://www.naih.hu/files/Privacy_Act-CXII-of-2011_EN_201310.pdf (ii)

The Hungarian National Authority for Data Protection and Freedom of Information (**NAIH**) is the body responsible for governing all matters pertaining to data protection and freedom of information in Hungary.

The NAIH operate as an independent state organ and hence their functions may only be determined by parliamentary acts.

(i)

Act CXII of 2011 on the Right of Informational Self-Determination and Freedom of Information is one of the most significant pieces of legislations in Hungary regarding data protection.

The scope of the Act is broad, applying to all data processing operations undertaken in Hungary, including:

1. Law enforcement
2. National security and defence sectors
3. Activities relating to the data of natural persons
4. Data in the public interest

Since the Act was first issued in 2011, the Hungarian Government has made substantial amendments to ensure it also implements the EU's General Data Protection Regulation (**GDPR**).

(ii)

Fraud

https://thb.kormany.hu/download/a/46/11000/Btk_EN.pdf (i)
https://corruptionprevention.gov.hu/ (ii)
https://integritashatosag.hu/en/ (iii)

Hungary's laws on fraud are enshrined within **Act C of 2012 on the Criminal Code**. This includes:

- **Section 373** – General Fraud
- **Section 374** – Economic Fraud
- **Section 375** – Information System Fraud (i)

Hungary's **National Anti-Corruption Programme** stipulates several key priorities in relation to tackling corruption and fraud in Hungary, including:

1. A focus on strengthening the anti-fraud and corruption guarantees to improve transparency in public procurement
2. Introducing training for participants involved in identifying violations of public procurement law, helping to prevent and detect fraud (ii)

The **Hungarian Integrity Authority** is responsible for preventing, detecting and correcting fraud, corruption and other irregularities that pose a threat to the financial interests of the EU. To achieve this, they cooperate with the European Anti-Fraud Office (**OLAF**), discussing ways of strengthening anti-fraud and corruption measures across EU borders.

(iii)

Commentary

Sanctions

https://www.mnb.hu/en/supervision/regulation/anti-money-laundering/economic-and-financial-sanctions

In accordance with the **MND Act**, the Central Bank of Hungary is the authority responsible for implementing sanctions in Hungary, in line with restrictive measures imposed by the **UN Security Council** and the **Council of the European Union.**

Terrorism

https://honvedelem.hu/hirek/government-resolution-1163-2020-21st-april.html (i)

https://www.mnb.hu/letoltes/aml-cft-act-hungary2020.pdf (ii)

In 2020, the Government of Hungary introduced **Resolution 1163/2020** on Hungary's **National Security Strategy of 2012.**

The strategy aims to identify appropriate responses to the ever-changing national security landscape, including a higher level of self-sufficiency in the field of counterterrorism. (i)

Act CXXXVI of 2007 on the Prevention and Combatting of Money Laundering and Terrorist Financing is a significant piece of legislation with regards to combatting terrorism in Hungary.

One of the main goals of the Act is to prevent the flow of funds and other financial means used in the financing of terrorism, covering a broad range of institutions and operators in Hungary. (ii)

Company Registrar

https://www.e-cegjegyzek.hu/ (i)

https://www.e-cegjegyzek.hu/?cegkereses (ii)

The Ministry of Justice Company Information and the Electronic Company Registration Service. (i)

The Hungarian business information search engine. (ii)

Access to Public Information

https://www.naih.hu/freedom-of-information (i)

https://www.naih.hu/files/Act-CXII-of-2011_EN_23June2016.pdf (ii)

The **NAIH** are the governing body responsible for ensuring the citizens of Hungary have freedom of information i.e. the right to access data of public interest.

All citizens can request access to public information, whether that be verbally, submitted in writing, or electronically, made directly to the government body/organization in question. (i)

Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information governs the enforcement of the right to access public information in Hungary. (ii)

Other

https://2015-2019.kormany.hu/en

https://www.mnb.hu/en/innovation-hub/

Website of the Hungarian Government. (i)

The MNB iNNOHUB is a regulatory sandbox where you can explore the Hungarian legislation, request advice directly from the regulator and others. (ii)

Posture Rating – Hungary

The PR value of **6.7** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	9	7	8	8	5	8	2	5	6	6	3

Hungary has adopted many EU processes, supporting regulations and laws that support the domains. However, we did observe the extension of some of processes with the provision of additional tools to support the domains e.g. within the company registrar domain.

NB: **The figure does not reflect the execution of any processes, laws or regulations**.

India (Republic of)

Commentary

Financial Regulatory Authority

https://www.rbi.org.in/home.aspx (i)
https://rbidocs.rbi.org.in/rdocs/Publicati-ons/PDFs/RBIA1934170510.PDF (ii)
https://www.sebi.gov.in/ (iii)

The Reserve Bank of India (**RBI**) is the Central Bank of India. It was established in 1935, pursuant to the **Reserve Bank of India Act, 1934.**

The Bank performs various functions, including:

1. Regulating the issuing of Bank notes and maintaining reserves to secure monetary stability
2. Operate the currency and credit system
3. Develop and implement a modern monetary policy framework to meet the challenges faced in the economy
4. Effectively balance the objectives of price stability and economic growth

The Reserve Bank's affairs are governed by a central board of directors. The board is **appointed by the Government** in keeping with the Reserve Bank of India Act.

The Board for Financial Supervision (**BFS**) was first established in 1994 as a committee of the Central Board of Directors of the Reserve bank of India.

The BFS's primary objective is to **strengthen the supervision and surveillance** of the financial sector in India, including commercial banks, financial institutions and non-banking finance companies. Some of their main duties include:

1. Restructuring the system of bank inspections
2. Off-site surveillance
3. Strengthening the role of statutory auditors
4. Improving internal defences of supervised institutions

(II)

The Securities and Exchange Board of India (**SEBI**) aims to protect the interests of investors in securities and promote the development of and to regulate the securities market and for associated matters. (iii)

The Indian **rupee** is the official currency of India.

AI Act / Policy

https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf (i)
https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf (ii)
https://www.aitf.org.in/ (iii)

At the time of writing there no specific codified laws, statutory rules or regulations that directly regulate AI.

Nevertheless, various frameworks are being formulated to guide the regulation of AI, including:

1. India's **National Strategy for Artificial Intelligence** was issued in 2018 by National Institute for Transforming India (NITI Aayog). (i)
2. **Responsible AI** #AIFORALL – Approach Document for India (Feb 2021) and presents 7 Ethical System Considerations. (ii)

The Indian Artificial Intelligence task force. (iii)

Commentary

Anti-Money Laundering

https://fiuindia.gov.in/files/AML_Legislation/pmla_2002.html (i)
https://enforcementdirectorate.gov.in/ (ii)

The Prevention of Money Laundering Act, 2002 (PMLA). (i)

The **Directorate of Enforcement** is a multi-faceted government body, mandated with investigating offences in relation to money laundering and violations of foreign exchange laws. (ii)

Bribery

https://www.indiacode.nic.in/bitstream/123456789/15302/1/pc_act,_1988.pdf

The **Prevention of Corruption Act, 1988** is a foundational piece of legislation in India regarding combatting corruption, governing against bribery in both the public and private sector.

Consumer Protection

https://consumeraffairs.nic.in/acts-and-rules/consumer-protection (i)
https://consumeraffairs.nic.in/sites/default/files/CP%20Act%202019.pdf (ii)
https://consumeraffairs.nic.in/about-us/about-dca (iii)
https://doca.gov.in/ccpa/ (iv)

There are multiple legislations in India pertaining to consumer protection, all of which can be downloaded from the Ministry of Consumer Affairs website. (i)

The most consequential piece of legislation is the **Consumer Protection Act, 2019.** The Act was introduced to tighten existing consumer protection legislation, implementing several new provisions, including:

1. The Establishment of the Central Consumer Protection Authority (**CCPA**)
2. Simplifying the dispute resolution process
3. Additional clause to the 'Unfair Trade Practice'
4. Inclusion of E-commerce and direct selling

(ii)

The **Department of Consumer Affairs** is responsible for the implementation of the Consumer Protection Act, along with various other legislations in relation to consumer affairs. (iii)

The **CCPA** were established, pursuant to the Consumer Protection Act, 2019, with primary objective of regulating matters pertaining to the violation of consumer's rights, unfair trade practices and false/misleading advertisements. (iv)

Cloud Policy

https://www.nic.gov.in/service/national-cloud/

The **Government of India's GI Cloud (Meghraj) Strategic Direction Paper** was issued in 2013. The purpose of the publication is to provide a roadmap for establishing and implementing the GI Cloud in India and the adoption of cloud computing more generally.

Data / Privacy

https://sansad.in/getFile/BillsTexts/LSBillTexts/Asintroduced/341%20of%202019As%20Int....pdf?source=legislation

The Data Privacy and Protection Bill, 2019.

VPNs are legal in India. However, VPN service providers must log VPN traffic and provide this information to the government upon request especially in matters that concern national security and preventing cybercrime.

Commentary

Fraud

https://www.rbi.org.in/commonman/english/scripts/Notification.aspx?Id=578 (i)
https://sfio.gov.in/ (ii)
https://www.mca.gov.in/content/dam/mca/pdf/Companies_Act_1956_13jun2011.pdf (iii)

It is the responsibility of individual banks to prevent fraudulent activities occurring, **the RBI** does issue guidance regarding fraud-prone areas and necessary measures and safeguards to help fraud. The RBI has issued a set of instructions for Commercial Banks (excluding RRBs) and Financial Institutions on how to appropriately **classify and report fraudulent activities.** (i)

The Serious Fraud Investigation Office (**SFIO**) are responsible for investigating and prosecuting complex corporate frauds in accordance with section 212 of the Companies Act 2013. (ii)

The **Companies Act, 2013** (most recently amended in 2020) is an important piece of legislation in relation to combatting corporate fraud in India. The Act aims to promote transparency, strengthen enforcement mechanisms and enhance corporate governance to help prevent and penalise fraud. (iii)

Terrorism

https://fiuindia.gov.in/index.html

The Financial Intelligence Unit - India (FIU-IND) was set by the Government of India vide O.M. dated 18th November 2004 as a central national agency responsible for receiving, processing, analysing and disseminating information relating to suspect financial transactions. FIU-IND is also responsible for coordinating and strengthening efforts of national and international intelligence, investigation and enforcement agencies in pursuing the global efforts against money laundering and financing of terrorism.

The FIU-IND *publishes a list of sanctions* imposed by the Indian Government and is an independent body reporting directly to the Economic Intelligence Council (EIC) headed by the finance minister.

Company Registrar

https://www.mca.gov.in/MinistryV2/incorporation_company.html (i)
https://www.mca.gov.in/content/mca/global/en/home.html (ii)

The Ministry of Corporate Affairs is where to register a new company in India. (i)
URL link for a search tool for the Indian company registrar. (ii)

Access to Public Information

https://www.nationalarchives.nic.in/about-rti-act

Right to Information Act 2005 mandates timely response to citizen requests for government information. The RTI Portal Gateway for citizens provides a quick search of information on the details of first Appellate Authorities, PIOs etc. amongst others, besides access to RTI related information / disclosures published on the web by various Public Authorities under the government of India as well as the State Governments.

Other

https://www.india.gov.in/

The National Portal of India provides a single-window access to information and services that are electronically delivered from all Government Departments.

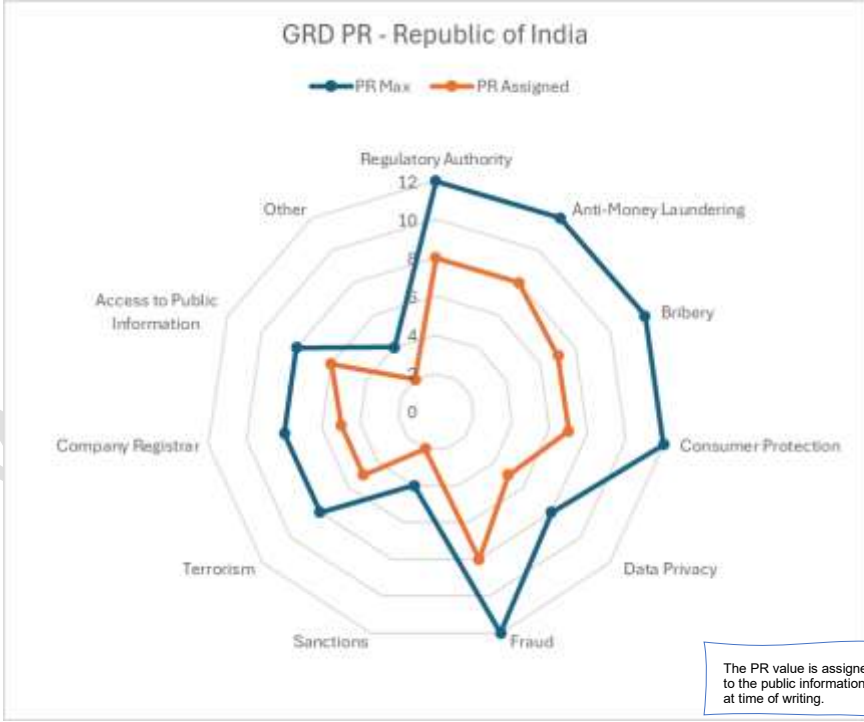
Posture Rating – India

The PR value of **6.3** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	8	8	7	7	5	8	2	5	5	6	2

India has many convoluted processes which seek to support the relevant domains. Domains are also supported by digital channels that provide additional supporting information for regulations which is reflected in the score assigned.

NB: **The figure does not reflect the execution of any processes, laws or regulations**.



Indonesia

Commentary

Financial Regulatory Authority

https://www.bi.go.id/en/default.aspx (i)
https://ojk.go.id/en/tentang-ojk/Pages/Visi-Misi.aspx (ii)

The **Bank Indonesia** is the central bank of Indonesia and mandated with one overarching goal, namely, to create and maintain stability of the national currency, which is achieved via the execution of the three core functions i.e. **Monetary, Stability** and **Currency Controls.**

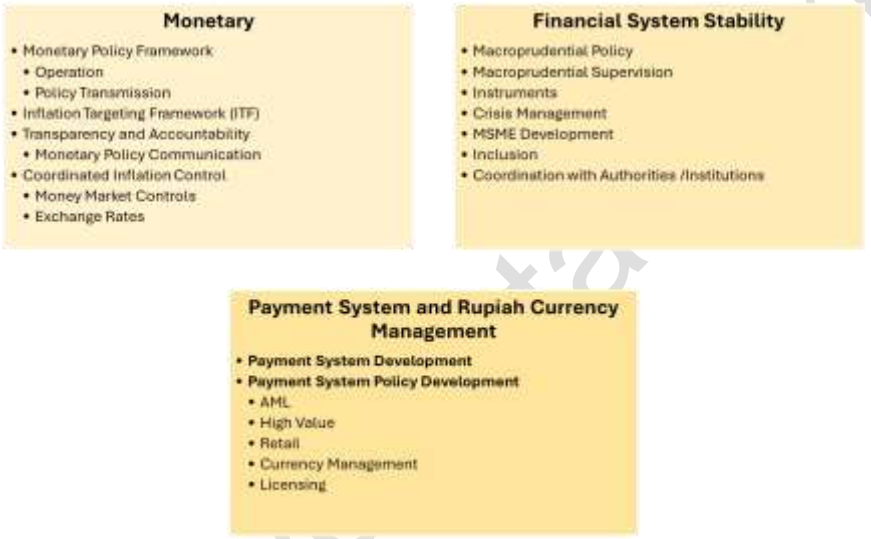


Figure 21 The Three Core Functions of Indonesian Central Bank

(i)

The Financial Services Authority (**OJK**) is a government agency, responsible for ensuring transparency, fairness and accountability within Indonesia's financial sector.

(ii)

The national currency of Indonesia is the **rupiah.**

AI Act / Policy

https://ai-innovation.id/strategi

The Indonesian National Strategy on Artificial Intelligence (Stranas KA) was launched on the commemoration of National Technology Awakening Day on August 10, 2020. (Currently not available in English)

Indonesia's **National AI strategy from 2020 to 2045** (also known as Stranas KA) was developed by the Ministry of Research and Technology and the National Research and Innovation Agency. The strategy was formulated with 5 key objectives:

1. Drive the *transformation* of Indonesia as an innovation-based country
2. *Promote* AI research and industrial innovation
3. *Improve* data and data-related infrastructure
4. *Implement* ethical and relevant AI policies
5. *Cultivate* a skilled AI workforce.

Commentary

Anti-Money Laundering

https://setkab.go.id/en/indonesia-becomes-full-member-of-fatf/#:~:text=As%20a%20result%20of%20the%20FATF%20Plenary%20in,said%20at%20the%20Merdeka%20Palace%2C%20Jakarta%2C%20Monday%20%2811%2F06%29. (i)

https://ojk.go.id/en/berita-dan-kegiatan/siaran-pers/Pages/OJK-Issues-New-Regulation-on-AML-CFT-and-CPF-Program.aspx (ii)

bi.go.id/en/fungsi-utama/sistem-pembayaran/anti-pencucian-uang-dan-pencegahan-pendanaan-terrorisme/Documents/SRA_ML_TF_PF_2022.pdf (iii)

https://www.ppatk.go.id/home/menu/2/profile.html (iii)

In 2023, Indonesia became the 40th member of the Financial Action Task Force (FATF). As such, Indonesia's Anti-Money Laundering (AML) polices are closely aligned with the **FATF's 40 recommendations**.

(i)

Prior to joining the FATF, the Indonesian Financial Services Authority (OJK) issued **Regulation (POJK) No. 12/POJK.01/2017** (amended in 2019) on the implementation of AML and Counter-terrorist Financing (CFT) in the financial services sector.

The aim of the regulation was to align Indonesia's policies more closely with the FATF's to gain full membership, focussing primarily on mitigating emerging risks of ML/FT.

(ii)

Bank Indonesia's AML/CFT framework aims to support the Indonesian Payment System (SPI) Vision of 2025, i.e. striking a balance between innovation and in the integrity of the payment system. The framework focuses on several areas, including:

1. Threats to economic stability and financial system integrity
2. Investment risks
3. Indonesia's international credibility

*Please note – URL responsiveness very slow outside of country.

(iii)

The Financial Transaction and Analysis Centre (**PPATK**) are Indonesia's Financial Intelligence Unit, playing a crucial role in preventing and eradicating ML offences.

In accordance with **Law No. 8 of 2010** on the Prevention and Eradication of Money Laundering, the PPAKT's position as an independent institution was strengthened, meaning other bodies are prohibited from interfering with their duties.

(iv)

Bribery

https://www.unodc.org/documents/indonesia/programme/PaparanStranas_english.pdf (i)

https://www.icj.org/wp-content/uploads/2013/01/Indonesia-Law-on-the-Commission-for-the-Eradication-of-Criminal-Acts-of-Corruption-2002-eng.pdf (i)

https://cacj-ajp.org/indonesia/legal-system/introduction/ (ii)

As a signatory of the UN Convention Against Corruption, Indonesia aims to seek to implement anti-bribery and corruption measures in line with the Convention's stipulated policy options and considerations. As such, they issued the **National Strategy for Corruption Prevention and Eradication (2012- 2025)**. (i)

Indonesia's Law No. **31 of 1999** on Eradication of Criminal Acts of Corruption, as amended by Law No. **20 of 2001.**

(ii)

With limited digital information we provide the URL for the ASEAN Judiciaries Portal (AJP) updated by the Indonesian ministry. (iii)

Commentary

Consumer Protection

https://bpkn.go.id/page/visi-dan-misi (i)
https://kadin.id/en/analisa/strategi-nasional-perlindungan-konsumen-2024-kini-meliputi-sektor-pariwisata-ekonomi-kreatif-dan-jasa-logistik/ (ii)

Indonesia's National Consumer Protection Agency (**BPKN**) is a government institution, established with the primary objective of helping consumers understand their rights and obligations. The BPKN seek to achieve the following missions:

1. Strengthen the legal and national consumer policy framework
2. Increase the efficiency of the consumer dispute resolution process
3. Expand access to consumer protection information and drive public awareness (i)

In 2024, the Government of Indonesia made amendments to the 2017 **National Strategy on Consumer Protection** through the issuance of **Regulation of the President No.49 of 2024**.

The main objective of the new strategy is to strengthen various functions of consumer protection by focussing on some of the following areas:

1. Accelerate the organization of consumer protection in certain priority sectors
2. Improving consumer capabilities with regards to understanding their rights and making optimal decisions
3. Boosting domestic demand

(ii)

Cloud Policy

https://ai-innovation.id/strategi

Whilst Indonesia does not have a standalone cloud policy. However, the National **AI Strategy recognises the importance of cloud computing** in boosting AI development and adoption. For example, of the key priorities within the strategy is to modernise Indonesia's current system infrastructure, including cloud computing, to ensure a unified national data system.

Data / Privacy

https://jdih.kominfo.go.id/produk_hukum/view/id/553/t/peraturan+menteri+komunikasi+dan+informatika+nomor+20+tahun+2016+tanggal+1+desember+2016

In 2016, the Minister of Communication and Information Technology issued the **Protection of Personal Data in Electronic Systems regulation**. This outlines various measures to ensure the collection and processing of personal data via electronic means is handled responsibly and securely e.g. Electronic Systems Operators are required to provide a consent form in Indonesian to request consent from personal data owners.

Fraud

https://iru.ojk.go.id/iru/BE/uploads/regulation/files/file_6e5d13f6-d310-4c27-9866-96993cd358b2-07122024112331.pdf

The OJK are the supervisory authority responsible for ensuring compliance with anti-fraud policies and regulation amongst financial service institutions (**LJKs**) in Indonesia.

In 2024, the OJK issued the regulation on the **Implementation of Anti-Fraud Strategies for Financial Services Institutions.** This was introduced primarily to cater for the increasing complexities of business activities carried out by LJKs, which have subsequently increased the risk of fraud.

The regulation aims to strengthen the internal control systems of LJKs, ensuring a standardised approach in the implementation of anti-fraud policies.

Commentary

Sanctions

https://www.ppatk.go.id/link/read/23/dttot-proliferasi-wmd.html (i)

The List of Suspected Terrorists and Terrorist Organizations (**DTTOT**) is the official sanctions list of Indonesia, implemented by PPATK.

Terrorism

https://www.bnpt.go.id/tupoksi (i)
https://www.ppatk.go.id/backend/assets/images/publikasi/1674614804_.pdf (ii)

The National Counter-Terrorism Agency (**BNPT**) is a non-ministerial government agency, responsible for formulating, coordinating and implementing national policies and regulations in the field of counterterrorism.

(i)

Law No. 9 of 2013 on the Prevention and Eradication of Terrorism Financing Crime is also a key piece of legislation with regards to combatting terrorism (specifically the financing of terrorism) in Indonesia.

(ii)

Company Registrar

https://www.ministryoflawandhumanrights.org/ (i)
https://ahu.go.id/pencarian/profil-pt (ii)

Companies in Indonesia can be registered via the Ministry of Law and Human Rights website full link for registration site not provided as unstable at time of writing

(i)

Link to search the company registrar.

(ii)

Access to Public Information

https://eppid.kominfo.go.id/storage/uploads/1_9_2-Undang_Undang_Nomor_14_Tahun_2008.pdf (i)
https://eppid.kominfo.go.id/daftar_informasi (ii)

Law No. 15 of 2008 on the Openness of Public Information stipulates the right of all Indonesian citizens to access public information i.e. any information produced, stored, managed, sent or received by a public agency.

(i)

The Ministry of Communication and Information (**PPID**) is the government body responsible for ensuring the transparency of public information in Indonesia.

(ii)

Other

https://indonesia.go.id/ (i)
https://www.dpr.go.id/en/index/link (ii)

The official Government website.

(i)

The House of Representatives website

(ii)

Posture Rating - Indonesia

The PR value of **5.9** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	8	8	6	6	6	7	2	5	5	4	2

Indonesia has introduced key processes to support the regulations and laws to address the domains and comply with its international obligations, many of which are available in the native language and reflected in the score.

As Indonesia introduces more digital channels, we expect the value to increase.

NB: **The figure does not reflect the execution of any processes, laws or regulations**.

The Islamic Republic of Iran

Commentary

Financial Regulatory Authority

https://www.cbi.ir/default_en.aspx

The Central Bank of Iran (**CBI**) also known as **BANK MARKAZI JOMHOURI ISLAMI IRAN** as stated in the Monetary and Banking Act of Iran (MBAI), is responsible for the design and implementation of the monetary and credit policies with due regard to the general economic policy of the country.

The major objectives of CBI as stated in the MBAI are:

1. Maintaining the value of national currency
2. Maintaining the equilibrium in the balance of payments
3. Facilitating trade-related transactions
4. Improving the growth potential of the country

The national currency of the Islamic Republic of Iran is the Iranian **rial**.

AI Act / Policy

https://tehrantimes.com/news/469628/Iran-plans-to-become-a-leading-country-in-AI

Limited Public Information available to sites outside of the Republic. However, Iran published the **National Strategy for Artificial Intelligence,** in 2019, aimed to promote and mobilize the wider society for education and research, innovation and development of AI-supported products and services in Iran – Document could not be sourced at time of publication.

On Jan 30th ,2022 the Tehran Times published an article entitled “Iran plans to become a leading country in AI” which provides insight into the plans of the Iranian Government (see URL).

Anti-Money Laundering

https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Call-for-action-october-2024.html (i)

https://www.unodc.org/islamicrepublicofiran/en/iran-to-strengthen-its-capacities-to-fight-money-laundering-and-financing-of-terrorism.html (ii)

Iran is classified as a high-risk jurisdiction according to the FATF. (i)

Iran received assistance from United Nations Office on Drugs and Crime (**UNODC**) to help strengthen its capacity to combat money laundering and the financing of terrorism. (ii)

Bribery

https://track.unodc.org/uploads/documents/UNCAC/WorkingGroups/ImplementationReviewGroup/10-14June2024/statements/Iran_statement_IRG15_agenda_item_2.pdf

The Islamic Republic of Iran does not have any standalone legislation specifically in relation to bribery. However, as a signatory of the United Nations Convention Against Corruption (**UNCAC**), Iran must seek to adopt measures as stipulated in the publication. For instance, Articles 15 and 16 of the Convention requests that state parties implement legislative measures against the bribery of national public officials, foreign public officials and international organizations.

Commentary

Consumer Protection	URL https://en-econom-ic.mfa.ir/en/cdk/func/getFile/file_ctp_id/602/file_id/184/file_field/cnt_file/file/Customer%E2%80%99s+right+protection+law.pdf/ Ministry of Commerce issued the **Customer's Right Protection Law.** This law covers the following areas: 1. **Duties of suppliers** of goods and services 2. Establishment of **Consumer Protection Associations** i.e. non-governmental, independent bodies whose main duties include consulting and cooperating with relevant organizations to improve customer rights; handling customer complaints and signposting them to relevant legal services. 3. Systems and processes for supporting **customer complaints** **Fines and punishments** for those in violation of customer protection law.
Cloud Policy	Navyan Abr Arvan Private Limited Company, known as Arvan Cloud, has played a prominent role in the Iranian government's development of the NIN infrastructure, a censored version of the Internet under the control of Iranian authorities and was deleted from the EU Sanctions list during 2024. ArvanCloud controls a significant percentage of Iran's cloud space market and continues to host many of the Islamic Republic's most important websites, including the Presidency, IRNA news agency and the Ministry of Islamic Guidance hence worthy of mention. Limited verified Information is available, however public links are available to the Arvan website. At the time of writing the Islamic Republic of Iran limits VPN access. While using a government-approved VPN is legal, these services are heavily **regulated and monitored**. Any attempt to use a non-approved VPN may result in up to a year in prison.
Data / Privacy	At the time of writing the Islamic Republic of Iran had not enacted any data protection legislations.
Fraud	No credible information available at time of writing.
Sanctions	URL https://sanctionlist.mfa.ir/ Individuals and entities in the sanction's list of the Islamic Republic of Iran.

Commentary

Terrorism

https://www.unodc.org/pdf/iran/drug_crime_situation/rule_of_law/crime_prevention/Terrorism.pdf

While there are no standalone laws in the Islamic Republic of Iran in relation to combatting terrorism, there are several laws and regulations that incorporate measures against terrorism and terrorist activities e.g. the **Islamic Penal Code** and the **Punishment of Misdemeanours and Crimes against Foreign Countries (1971).**

The **Coordinating National Committee** was established with the aim of implementing **UN Resolution 1373**, a counter-terrorism measure.

The Ministry of Foreign Affairs is responsible for reporting to the Counter-Terrorism Committee. Additionally, they work in collaboration with other Government ministries and agencies to prepare reports on the implementation of the UN Security Council's Resolutions.

Company Registrar

One is unable to search for free the Iran Company Register, which must be undertaken through a 3rd party.

No trusted sources determined at time of writing.

Access to Public Information

https://geneva.mfa.gov.ir/portal/newsview/704423/The-Islamic-Republic-of-Iran-Charter-on-Citizens%E2%80%99-Rights%C2%A0-December-2016

The Islamic Republic of Iran **Charter on Citizen's Rights (2016)** stipulates the right of Iranian citizens to access information.

Other

https://irangov.ir/en

The official Government website.

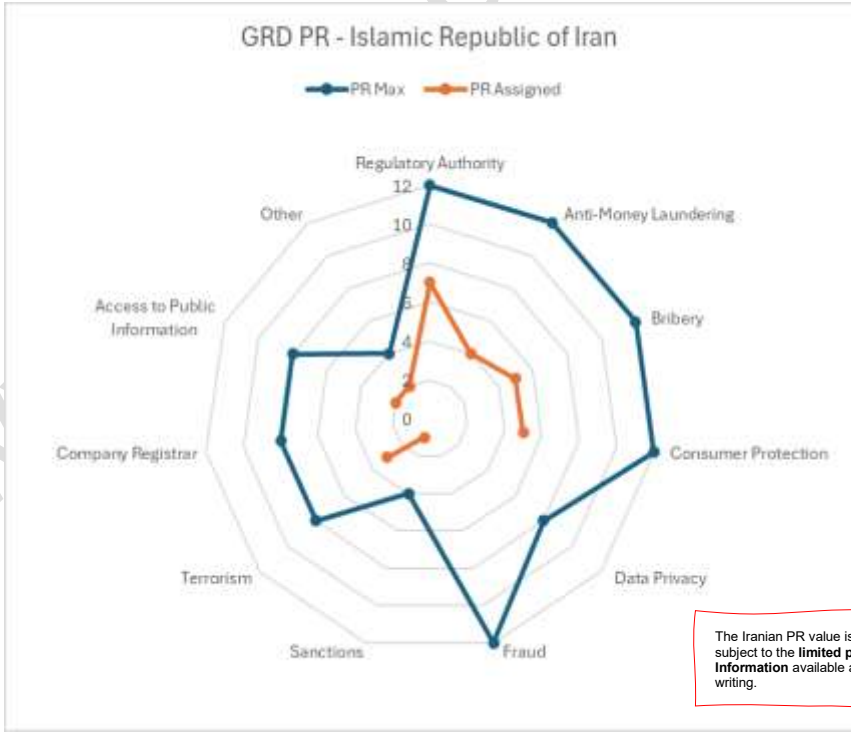
Posture Rating - Iran

The PR value of **2.9** is derived using the following **limited** assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	7	4	5	5			1	3		2	2

Due to Internet restrictions, both in and out, of Iran a true reflection of posture cannot be determined and hence limited values have been assigned. This will be updated as and when new data is available.

NB: **The figure does not reflect the execution of any processes, laws or regulations**.



The Iranian PR value is assigned subject to the **limited public Information** available at time of writing.

Ireland (Republic of)

Commentary

Financial Regulatory Authority

https://www.centralbank.ie/ (i)
https://www.centralbank.ie/regulation/how-we-regulate (ii)

The Central Bank of Ireland (**CBI**) is the Irish member of the Eurosystem.
The Bank's primary mission is to maintain monetary and financial stability, whilst also ensuring that the financial system serves the best interests of consumers and the wider economy.

(i)

The CBI regulates the financial sector of Ireland with the following **overarching objectives**:

1. Ensure stability of the financial system
2. Implement comprehensive regulation of financial institutions and markets
3. Restructuring of credit institutions

To achieve these objectives, the CBI implements various **measures**, including:

1. Rigorous authorisation procedures
2. Assessment of applications for approval of persons in accordance with fitness and probity standards
3. Developing financial regulation policy
4. Assertive risk-based approach to supervision and credible threat enforcement

(ii)

The **euro** is the official currency of the Republic of Ireland.

AI Act / Policy

https://www.gov.ie/en/press-release/c7fd8-ministers-welcome-adoption-of-eu-artificial-intelligence-ai-act/ (i)
https://enterprise.gov.ie/en/publications/publication-files/national-ai-strategy.pdf (ii)
https://www.gov.ie/en/publication/8cae9-enterprise-digital-advisory-forum/ (iii)
https://www.gov.ie/en/press-release/51b459-minister-odonovan-launches-govtech-report/ (iv)

Ireland is an EU Member State and as such, seeks to adopt the EU Artificial Intelligence Act.

(i)

The Government of Ireland also issued the country's **National AI Strategy, 'AI – Here for Good'.**
To implement the strategy, a range of Government Departments, State agencies and other bodies have been selected to fulfil its strategic objectives.

(ii)

The Enterprise Digital Advisory Forum (**EDAF**) was established as part of the Strategy, bringing together enterprise experts to help drive the digitalization of enterprise across Ireland.

(iii)

Another group established off the back of the Strategy is the **GovTech Delivery Board.**
The GovTech report of 2019 outlines a focus on applying emerging technologies such as AI to help drive efficiencies and lower costs of public services in Ireland.

(iv)

Commentary

Anti-Money Laundering

https://www.centralbank.ie/regulation/anti-money-laundering-and-countering-the-financing-of-terrorism/regulatory-requirements-guidance (i)

https://www.amlcompliance.ie/about-us/ (ii)

The Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (**CJA**), most recently amended in 2018, is the most consequential piece of legislation in Ireland pertaining to Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT).

The CJA incorporates various relevant **EU legislations**, including:

1. The third Anti-Money Laundering Directive (**2005/60/EC**) and its Implementing Directive (2006/70/EC)
2. The fourth Anti-Money Laundering Directive ((**EU) 2015/849**)

Additionally, the Act also seeks to encompass the recommendations set out by the Financial Action Task Force (**FATF**).

In accordance with the CJA, the **CBI are the governing body responsible** for monitoring and supervising financial and credit institutions regarding compliance with their AML/CFT obligations.

(i)

Another player in relation to enforcing AML/CFT laws in Ireland is the Anti-Money Laundering Compliance Unit (**AMLCU**).

The AMLCU is responsible for supervising authorities that are not already under the supervision of another competent authority. This might include:

- High value goods dealers
- Tax advisors
- External accountants

(ii)

Bribery

https://www.anticorruption.ie/about-us/

There are multiple departments within Ireland's Government responsible for developing and implementing anti-bribery and corruption polices, for instance:

1. The **CBI**
2. The Garda National Economic Crime Bureau (**GNECB**)
3. The Standards in Public Office Commission (**SIPOC**)
4. Tribunals of inquiry, commissions on investigation and inspectors

Ireland is also party to various international anti-corruption groups, including:

- The United Nations Convention Against Corruption (**UNCAC**)
- The **OECD Convention** on Combatting Bribery of Public Officials in International Business Transactions

As such, Ireland is subject to monitoring and peer-review in association with the above instruments.

Commentary

Consumer Protection

https://www.irishstatutebook.ie/eli/2022/act/37/enacted/en/html (i)
https://www.ccpc.ie/business/ccpc-welcomes-new-rights-for-consumers/ (ii)
https://www.ccpc.ie/ (iii)

The **Consumer Rights Act** was enacted in 2022, simplifying and updating existing consumer protection law in Ireland.

(i)

The Act brought in several key changes, including:

1. Stronger rights regarding faulty goods e.g. introduction of a 30-day cancellation period
2. More accountability for service providers
3. Ban on fake reviews
4. New transparency requirements for online marketplaces
5. Protection for consumers of digital content services

(ii)

The Competition and Consumer Protection Commission (**CCPC**) is the governing body responsible for ensuring compliance with competition and consumer protection law in Ireland.

The main goal of the CCPC is to improve market conditions for consumers. They aim to achieve this by performing the following functions:

1. Influence policy and public debate
2. Raise public awareness of the importance of open and competitive markets
3. Provide consumers with information about their rights, personal finance and product safety

(iii)

Cloud Policy

https://www.ogcio.gov.ie/71/4468be59812f40dda7003116cf05f196_1.pdf (i)
https://assets.gov.ie/214584/fa3161da-aa9d-4b11-b160-9cac3a6f6148.pdf (ii)

The **Cloud Computing Advice Note** was issued in 2019, with the aim of providing comprehensive guidance for organizations in relation to the adoption of cloud services.

The overarching goal of the Note is to ensure the Government follows a **'cloud-first'** approach for all new systems and that existing Government systems move towards a **hybrid-cloud environment.**

(i)

Cloud computing also features heavily in Ireland's 'Harnessing Digital – The Digital Ireland Framework'.

One of the key targets within the framework is for 75% of enterprises to take-up Cloud Computing, Big Data and or AI by 2030, with a particular **focus on digitalising SMEs**.

The **Civil Service Renewal Strategy 2030** also stipulates plans to take a 'cloud-oriented' approach in its delivery of services.

(ii)

Commentary

Data / Privacy

https://www.dataprotection.ie/en/who-we-are/data-protection-legislation (i)
https://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html (ii)

The Data Protection Commission (**DPC**) are governed by numerous legislative frameworks, including:

- The EU's General Data Protection Regulation (**GDPR**)
- Data Protection Act 2018 (i)

On a national level, the **Data Protection Act 2018** is the most consequential piece of legislation in Ireland pertaining to data protection.

Whilst the GDPR covers the fundamentals of data protection in Ireland, the Data Protection Act of 2018 also outlines various **additional requirements/regulations** concerning data protection e.g. reasons for and the extent to which, data subject rights may be restricted.

(ii)

Fraud

https://www.irishstatutebook.ie/eli/2021/act/2/enacted/en/html?q=fraud

In 2021, the **Criminal Justice (Theft and Fraud Offences) (Amended) Act** was issued, with the aim of ensuring companies have the appropriate systems and controls in place to effectively prevent and detect fraud and corruption in Ireland.

The Act focuses particularly on businesses that operate within Europe/attract EU funding and even introduces a new specific offence of **'fraud impacting the financial interests of the EU'.**

Sanctions

https://www.centralbank.ie/regulation/how-we-regulate/international-financial-sanctions

The CBI are responsible for enforcing financial sanctions in Ireland. These are in line with both the EU and UN's consolidated Sanctions Lists.

Terrorism

https://www.irishstatutebook.ie/eli/1939/act/13/enacted/en/html (i)
https://www.irishstatutebook.ie/eli/2005/act/2/enacted/en/htm (ii)

The most significant piece of legislation in Ireland pertaining to countering terrorism on a domestic level is the **Offences against the State Acts 1939-1998**. This focuses on regulating against 'actions and conduct calculated to undermine public order and the authority of the state'.

(i)

In relation to combatting international terrorism, the **Criminal Justice (Terrorist Offences) Act** was issued in 2005. This Act aims to fulfil Ireland's duties as member of the EU and UN, implementing several international instruments directed towards counterterrorism.

(ii)

Commentary

Company Registrar

https://www.cro.ie/en-ie/ (i)
https://core.cro.ie/ (ii)

Companies Registration Office (**CRO**) Ireland.

(i)

The CRO also offers a search solution for the company registrar.

(ii)

Access to Public Information

https://www.irishstatutebook.ie/eli/2014/act/30/enacted/en/html (i)
https://foi.gov.ie/guidance/about/ (ii)

In accordance with the **Freedom of Information Act 2014**, all Irish citizens have the right to access records held by Freedom of Information (**FOI**) bodies.

(i)

To gain access to information, citizens must apply directly to the relevant public body, as opposed to the Freedom of Information Central Policy Unit (**CPU**).

(ii)

Other

https://www.gov.ie/en/

The Irish government website which provides a search capability for government services and miscellaneous information.

Posture Rating - Republic of Ireland

The PR value of **6.8** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	9	8	8	7	6	8	2	6	6	5	3

The Republic of Ireland, as a member of the EU, has adopted and extended the processes, regulations and laws which address both domain management and any international obligations.

NB: **The figure does not reflect the execution of any processes, laws or regulations**.

The PR value is assigned subject to the information available at time of writing.

Israel (State of)

Commentary

Financial Regulatory Authority

https://www.boi.org.il/en/ (i)
https://www.boi.org.il/en/bank-of-israel/about-the-bank-of-israel/ (ii)
https://www.gov.il/en/pages/about_mof (iii)
https://www.gov.il/en/departments/israel_securities_authority/govil-landing-page (iv)

The Bank of Israel is the central bank of the State of Israel. The Bank was established in 1954.

(i)

The Bank is fully independent in its operations and is governed by the **Bank of Israel Law, 5770-2010.** Its main objectives are as follows:

1. Maintain price stability
2. Support the objectives of the Government's economic policies
3. Support the stability and overall functioning of the financial system

(ii)

The **Ministry of Finance** is the governing authority responsible for regulating Israel's insurance, pension and capital markets (amongst many other duties and responsibilities).

(iii)

The Israel Securities Authority (**ISA**) is another key financial regulatory authority in Israel. They carry out various functions, including, supervising and regulating the mutual funds sector and monitoring reports of relevant corporations.

(iv)

AI Act / Policy

https://www.gov.il/en/pages/ai_2023 (i)
https://www.gov.il/BlobFolder/policy/ai_2023/en/Israels%20AI%20Policy%202023.pdf (ii)

Israel's **Ministry of Innovation, Science and Technology** collaborated with the Ministry of Justice to develop Israel's first comprehensive AI policy.

The aim of the policy is to promote responsible AI innovation and development, whilst also addressing concerns related to bias, transparency, safety, accountability and privacy.

(i)

'Israel's Policy on Artificial Intelligence – Regulation and Ethics' can be accessed via the Ministry of Innovation, Science and Technology's website.

Some of the key policy principles/recommendations outlined in the publication are as follows:

1. Adopting regulations across a wide range of sectors.
2. Aligning its regulatory approach with leading countries and international organizations e.g. the OECD
3. Adopting a risk-based approach to AI development and adoption
4. Promoting cooperation between the *public* and *private* sectors

(ii)

Commentary

Anti-Money Laundering

https://www.gov.il/en/departments/impa/govil-landing-page (i)
https://www.gov.il/en/pages/aml-regime (ii)

Israel's Financial Intelligence Unit (FIU), otherwise known as the Israel Money Laundering and Terror Financing Prohibition Authority (**IMPA)** were first established in 2002, pursuant to the **Prohibition of Loney Laundering Law, 2000.**

The IMPA is an independent body leading on combatting money laundering and terrorist financing (AML/CFT) in Israel. Furthermore, they coordinate Israel's global AML/CFT efforts in line with international standards established by the FATF.
(i)

The Prohibition of Money Laundering Law, 5760-2000 (**PMLL**) is the most significant piece of legislation Israel regarding their AML regime.

The PMLL covers 4 main areas:

1. Preventative measures e.g. obligations of financial institutions to appoint a corporate compliance officer.
2. Imposing criminal sanctions on money-laundering associated offences.
3. Confiscating 'prohibited property'.
4. Establishing the IMPA and granting them power to share intelligence information with foreign FIUs.

(ii)

Bribery

https://www.gov.il/en/pages/corruption_fight

Israel is party to various **international instruments** in relation to combatting bribery and corruption, including:

- The UN Convention against Corruption.
- The OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions.

Israel has also made a range of commitments on a domestic level to help strengthen its bribery and corruption policies. For example, in 2008 an additional bribery offence was introduced to the Israeli Penal Code under Article 291A, criminalizing the **offence of bribery to a foreign public official**.

Commentary

Consumer Protection

https://www.gov.il/en/service/filing_a_complaint_to_fair_trade_authority (i)
https://www.gov.il/BlobFolder/generalpage/general_tuota/he/EN_Brushur_SITE.PDF (ii)

The Consumer Protection and Fair-Trade Authority (**CPFTA**) is an independent government body responsible for enforcing consumer protection regulation, pursuant to the **Consumer Protection Law, 1981.**

(i)

The CPTFA performs various functions, including but not restricted to:

1. Investigating companies and businesses who are suspected to be in violation of consumer protection law and imposing relevant administrative sanctions where necessary
2. Handling all public inquiries in relation to consumer protection via the designated service centre
3. Developing and updating consumer protection legislation
4. Informing and educating businesses and consumers on consumer protection law

(ii)

Cloud Policy

https://www.gov.il/en/departments/topics/nimbus_cloud_strategy/govil-landing-page (i)
https://www.gov.il/en/pages/aboutnimbus (ii)

The Israeli Governments Cloud Strategy, otherwise known as the **'Nimbus Project'**, provides a comprehensive framework for activities in relation to cloud computing.

The strategy focuses on several key areas, including:

1. Increasing the **efficacy** of Government policy
2. Accelerating **innovation**
3. Promoting economic **efficiency**
4. Maximising technological **flexibility**
5. Improving cyber defence and data **security**

(i)

The Nimbus Project was established with the aim of resolving some of the issues that arise because of the legal and administrative complexities that come with public cloud infrastructures.

The project aims to achieve various objectives, including:

- Significant **improvements** to Government work processes and public services
- **Accelerating** the Government's digital transformation process
- Improve command, control and cyber defence **capabilities**

(ii)

Commentary

Data / Privacy

https://www.gov.il/en/pages/about_ppa (i)
https://www.gov.il/BlobFolder/legalinfo/legislation/en/ProtectionofPrivacyLaw57411981unofficialtranslatio.pdf **(unofficial translation)** (ii)

The Privacy Protection Authority (**PPA**) is an independent government agency, responsible for enforcing provisions regarding data protection and providing various enforcement tools to the Registrar.

The PPA enforces data protection regulation across all sectors, both public and private, in accordance with the Privacy Protection Law.

(i)

The Protection of Privacy Law, 5741- 1981 **(PPL**) is the most consequential piece of legislation in Israel pertaining to data protection. The Law covers a range of areas, including:

- Defining what classifies as an infringement of data privacy
- Effectively managing and utilising databases to protect the privacy of personal data
- Mitigating potential threats to data privacy

(ii)

Fraud

https://www.gov.il/he/pages/relevant-legislation-01

Israel legislates against fraud in the public sector under **Section 284 of the Penal Law, 5737-1977 – Fraud and Breach of Trust.** This states that any public servant who has committed fraud or shows a breach of trust that harms the public interest is liable to three years imprisonment.

Sanctions

https://nbctf.mod.gov.il/en/Minister%20Sanctions/Designation/Pages/IsraeliSanctionsRegime.aspx

The Israeli Sanctions Regime (including the designated list of terrorist organizations and unauthorized associations files).

Terrorism

https://www.gov.il/BlobFolder/dynamiccollectorresultitem/counter-terrorism-law-2016-english/he/legal-docs_counter_terrorism_law_2016_english.pdf
unofficial translation (i)
https://nbctf.mod.gov.il/en/Pages/default.aspx (ii)

In 2016, the Government of Israel issued the **Counter-Terrorism Law, 5776-2016.** The purpose of the Law is to provide a comprehensive framework for combatting terrorism in Israel, outlining relevant legal and criminal provisions. This also includes stipulating the powers of special enforcement powers in preventing and foiling terrorist offences.

(i)

The National Bureau for Counter Terror Financing of Israel (**NBCFT**) is a sub-department of the Ministry of Defence, responsible for developing national enforcement policies, directed at combatting terrorist financing and the proliferation of weapons and mass destruction.

(ii)

Commentary

Company Registrar

https://www.gov.il/en/departments/topics/registrar_of_companies/govil-landing-pagez (i)

https://ica.justice.gov.il/GenericCorporarionInfo/SearchCorporation?unit=8 (ii)

The company registration section of the government website.

(i)

It is possible to conduct extremely specific searches through the Israeli Corporations Authority.

(ii)

Access to Public Information

https://www.gov.il/he/pages/klali09 (i)

https://forms.gov.il/globalData/GetSequence/gethtmlform.aspx?formType=hofeshmeyda%40justice.gov.il (ii)

The **Freedom of Information Law, 5758-1998** stipulates that all Israeli citizens/residents have the right to receive information held by public authorities, if information does not harm another interest e.g. national security, personal privacy etc.

(i)

Information can be requested via the Ministry of Justice – Freedom of Information website.

(ii)

Other

https://www.gov.il/en

The Israeli government services website.

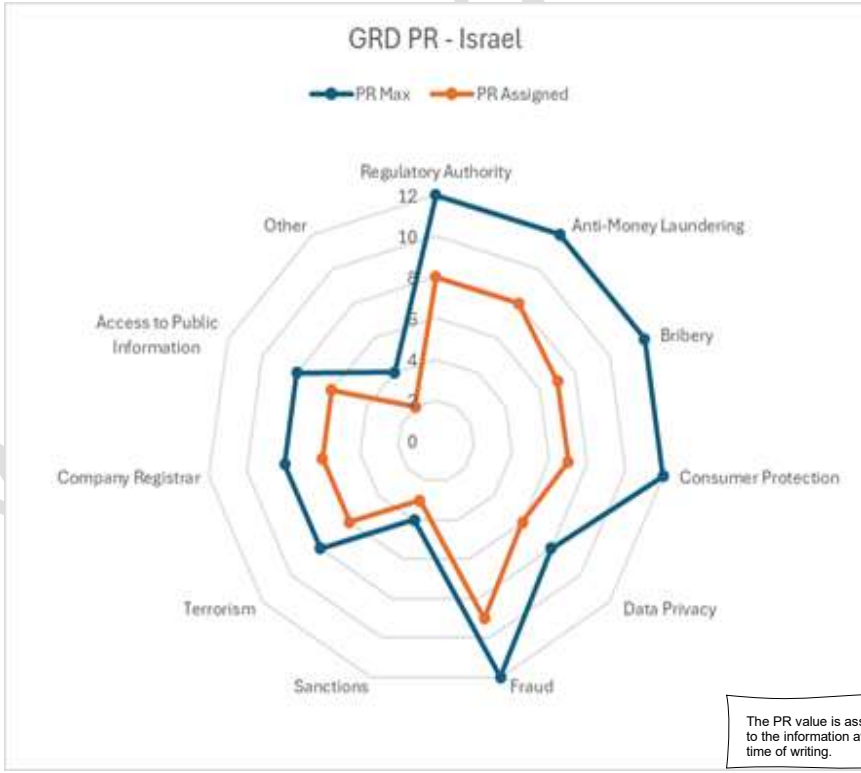
Posture Rating Israel

The PR value of **6.8** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	8	8	7	7	6	9	3	6	6	6	2

Israel has created, adapted and matured several processes, regulations and laws with impressive technology enablers to support domains and simplify compliance.

NB: **The figure does not reflect the execution of any processes, laws or regulations**.



The PR value is assigned subject to the information available at the time of writing.

Isle of Man

Commentary

Financial Regulatory Authority

https://www.gov.im/about-the-government/statutory-boards/isle-of-man-financial-services-authority/ (i)
https://www.gov.im/categories/tax-vat-and-your-money/manx-currency-coins-and-notes/ (ii)

The Isle of Man Financial Services Authority **("the Authority**") was first established in 2015, pursuant to the **Transfer of Functions Order, 2015.**

The Authority performs a range of functions, including:

1. Regulating and supervising financial activities/instruments e.g. deposit taking, investment business, collective investment schemes, retirement benefit schemes etc.
2. Conducting investigations into AML/CFT violations.
3. Overseeing directors and persons responsible for management, administration or affairs of commercial entities.
4. Participating in consultations, working groups and other arrangements.

(i)

Whilst the Isle of Man is a British Island, it still has a high degree of **economic and fiscal independence.** For example, it has its own government, makes its own laws and has autonomy over its taxes and expenditure.

(ii)

The national currency in the Isle of Man is the **Manx pound,** which has parity with the British pound.

AI Act / Policy

https://www.iomdfenterprise.im/media/scpn4mwx/web-digital-iom-programme-2024.pdf

The **Digital Isle of Man Programme** was first launched in 2024.

AI is a cornerstone of this programme, with a key objective of achieving a 10% increase in the Isle of Man's GDP by 2030 by fully leveraging the potential of AI.

There are several polices in place to help achieve this objective, including:

1. Developing an AI strategy for up to the year 2030.
2. Developing a five-year AI-centred delivery plan and securing necessary funding to implement it.
3. Seeking out AI regulatory opportunities.

Anti-Money Laundering

https://www.gov.im/about-the-government/departments/home-affairs/executive-office/anti-money-laundering-legislation-and-countering-the-financing-of-terrorism-amlcft/ (i)

https://www.gov.im/media/470621/anti-moneylaunderingandcounteringthefinancingofterrorismcode2019.pdf (ii)

https://www.iompolice.im/footer/corporate/economic-crime-unit/ (iii)

The **Anti-Money Laundering and Countering the Financing of Terrorism Code 2019** is the most significant piece of legislation in the Isle of Man pertaining to combatting money laundering and terrorist financing.

A primary objective of this legislation is to bring the Isle of Man into closer alignment with international best practices and ensure full compliance with **FATF recommendations.**

In accordance with the 2019 Code, all departments within the Isle of Man's Government must **publish three lists** containing entities that are of varying risk-levels regarding ML/TF. The three categories are as follows:

- List A – ***Highest*** threat of ML/TF. Includes jurisdictions where the FATF have requested countermeasures be imposed.
- List B – ***Moderate*** risk of ML/TF. Jurisdictions with significant AML/CFT deficiencies.
- List C – ***Jurisdictions*** that operate roughly in line with standards set by the IOM.

(i)

Full version of the legislation is available on the Department of Home Affairs' website.

(ii)

The Isle of Man Constabulary also has a dedicated **Economic Crime Unit**. This group carries out a range of duties, including investigating and raising awareness of economic crimes such as ML/TF.

(iii)

Commentary

Bribery

https://www.gov.im/about-the-government/departments/cabinet-office/amlcft-policy-office/anti-bribery-and-corruption-project/ (i)

https://www.gov.im/media/1377163/2022-gd-0055.pdf (ii)

https://www.gov.im/about-the-government/departments/the-treasury/audit-advisory-division/ (iii)

The AML/CFT Office of the Isle of Man developed the **Anti-Bribery and Corruption Project** to address bribery and corruption both domestically and internationally. The project aims to identify potential gaps in existing measures and additionally, provide recommendations to mitigate associated risks.
(i)

In 2022, the Government of the Isle of Man issued the **Anti-Bribery and Corruption Strategy** for the years 2022-2027.

The strategy addresses bribery and corruption in the public and private sector, targeted at both organizations and individuals. There are five overarching objectives that form the basis of the Strategy. These are as follows:

1. Identify the main bribery and corruption risks via the National Risk Assessment.
2. Mitigate vulnerabilities to bribery and corruption in the public sector.
3. Implement a comprehensive approach to combatting bribery on both a national and international level.
4. Improve detection, reporting and enforcement of bribery and corruption.
5. Deliver a long-term, sustainable model for addressing ongoing risks of bribery and corruption.

(ii)

The **Audit Advisory Division of the Treasury** is instrumental in the Isle of Man's efforts to combat bribery and corruption. A key responsibility of the division is to assess the effectiveness of government processes designed to address these issues.

(iii)

Consumer Protection

https://legislation.gov.im/cms/images/LEGISLATION/PRINCIPAL/2016/2016-0006/2016-0006_1.pdf (i)

https://www.gov.im/categories/tax-vat-and-your-money/consumer-advice (ii)

The **Consumer Protection Act 1991** (most recently amended in 2016) is the most significant piece of legislation in the Isle of Man pertaining to consumer protection. This covers various topics, including:

1. Product liability
2. Provisions regarding the safety of consumers
3. Misleading price indicators and advertisements
4. Unfair consumer contracts
5. Rights of consumers in relation to high-purchase motor vehicles

(i)

The **Isle of Man Office of Fair Trading** provide consumers with advice on their rights when purchasing goods and services. Furthermore, they are responsible for enforcing criminal consumer protection legislation and providing guidance on civil consumer legislation.

(ii)

Commentary

Cloud Policy

URL https://www.iomdfenterprise.im/media/scpn4mwx/web-digital-iom-programme-2024.pdf

Whilst cloud computing is not currently incorporated into the Isle of Man's **digital programme**, there are various plans mentioned regarding future implementation. For example, introducing pervasive cloud i.e. exploring cloud-computing as a driver for business innovation.

Data / Privacy

URL https://www.gov.im/about-the-government/data-protection-gdpr-on-the-isle-of-man/ (i)

https://legislation.gov.im/cms/images/LEGISLATION/PRINCIPAL/2018/2018-0010/2018-0010_2.pdf (ii)

https://www.inforights.im/ (ii)

Europe's General Data Protection Law (**GDPR**) has been integrated into the Isle of Man's data protection law, pursuant to an Order made under the **Data Protection Act 2018.**

The GDPR and LED Implementing Regulations 2018 is a set of data protection provisions, outlining relevant data protection procedures in line with European law and the powers of the **Information Commissioner**, i.e. crime prevention, investigation and law enforcement.

(i)

The full version of the Data Protection Act 2018 is available to download from the Government's website.

(ii)

The Isle of Man **Information Commissioner** performs various functions in relation to data protection. These include:

1. Maintaining a register of data controllers who have declared the processing of personal data.
2. Promoting good practice amongst data controllers and offering guidance and support.
3. Conducting assessments of personal data processing upon the request of either an individual or the data controller.

(ii)

Commentary

Fraud

https://www.legislation.gov.im/cms/images/LEGISLATION/PRINCIPAL/2017/2017-0007/2017-0007.pdf (i)

https://www.gov.im/media/1377163/2022-gd-0055.pdf (ii)

https://www.iompolice.im/footer/corporate/economic-crime-unit/ (iii)

https://www.gov.im/about-the-government/departments/the-treasury/audit-advisory-division/ (iv)

The **Fraud Act 2017** is one of the most consequential pieces of legislation in the Isle of Man pertaining to fraud, covering the following:

- Defining the various types of fraud e.g. fraud by false representation, fraud by failing to disclose information etc. and the penalties in place for those convicted.
- Obtaining services dishonestly and the penalties in place for those convicted.
- Fraud committed outside of the Isle of Man's jurisdiction.

(i)

Fraud is defined as one of the *categories of corruption* in the **Anti-Bribery and Corruption Strategy 2022-2027**. The Government classifies it as 'the act of intentionally and dishonestly deceiving someone in order to gain an unfair or illegal advantage (financial, political or otherwise').

(ii)

The Isle of Man Constabulary's **Economic Crime Unit** is responsible for investigating serious and complex fraud cases (amongst other economic crimes), leveraging financial and other intelligence to combat criminal activity.

(iii)

The **Treasury, Audit Advisory Division** also play an important role in combatting financial crimes such as fraud in the Isle of Man. They are responsible for evaluating the efficacy of government processes in relation to fraud, bribery and corruption.

(iv)

Sanctions

https://www.gov.uk/government/publications/the-uk-sanctions-list (i)

https://www.gov.im/sanctions-and-export-control (ii)

The Isle of Man is bound by the **UK Sanctions List**.

(i)

The **Customs and Immigration Division** is the regulatory authority responsible for implementing UN and UK sanctions in the Isle of Man. Additionally, they are responsible for:

1. Publishing sanctions designation updates and guidance.
2. Promoting compliance and preventing breaches of sanctions law.

(ii)

Commentary

Terrorism

https://legislation.gov.im/cms/images/LEGISLATION/PRINCIPAL/2003/2003-0006/2003-0006_4.pdf (i)

https://www.gov.im/about-the-government/departments/home-affairs/executive-office/anti-money-laundering-legislation-and-countering-the-financing-of-terrorism-amlcft/ (ii)

The **Anti-Terrorism and Crime Act 2003** defines terrorism as *any action designed to influence the government or international government organization or intimidate the public or a section of the public*. Furthermore, these actions are driven by the motive of advancing a *political, religious, racial or ideological cause*.

The Act covers a wide range of areas, including:

1. Proscribed organizations i.e. groups that have been identified as being linked to terrorism
2. Terrorist property
3. Notification requirements
4. Terrorist investigations
5. Counter-terrorist power

(i)

AML/CFT legislation, for example, the **Anti-Money Laundering and Countering the Financing of Terrorism Code 2019** also plays a crucial role in combatting terrorism in the Isle of Man. The primary aim of the Code is to prevent the financial system from being exploited for the means of activities such as the financing of terrorism.

(ii)

Company Registrar

https://www.gov.im/categories/business-and-industries/companies-registry (i)

https://services.gov.im/ded/services/companiesregistry/companysearch.iom (ii)

The official website of the Isle of Man Government, where one can register a company.

(i)

URL for the company search capability (ii)

Access to Public Information

http://www.legislation.gov.im/cms/images/LEGISLATION/PRINCIPAL/2015/2015-0008/2015-0008_1.pdf (i)

https://services.gov.im/freedom-of-information/ (ii)

The **Freedom of Information Act 2015** enables residents of the Isle of Man to access information held by public authorities.

(i)

Public information can be requested via the Isle of Man's Government website.

(ii)

Other

https://www.gov.im/

The official Isle of Man Government website.

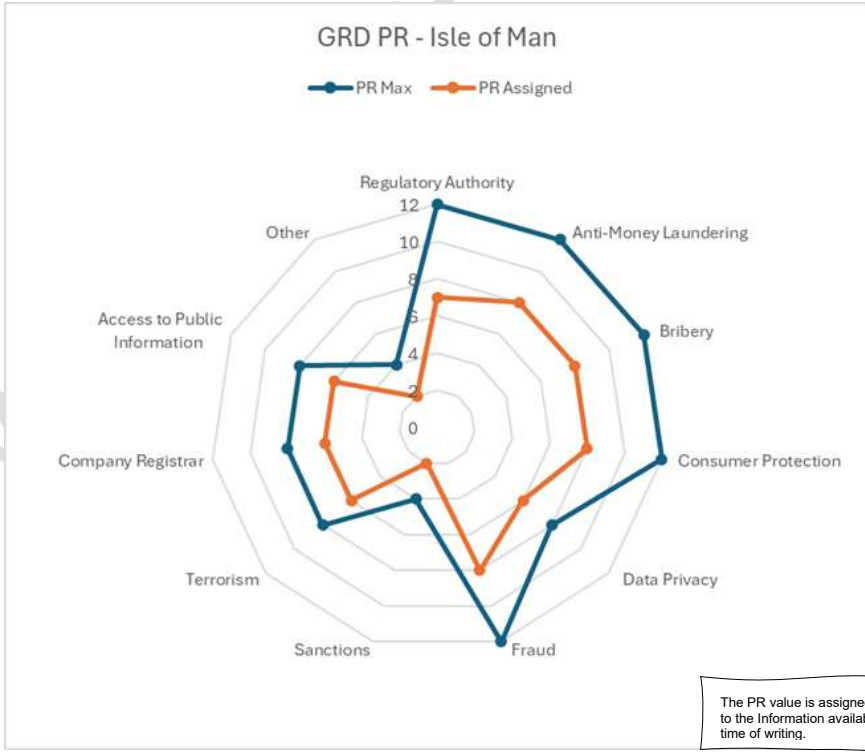
Posture Rating Isle of Man

The PR value of **6.7** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	7	8	8	8	6	8	2	6	6	6	2

The Isle of Man has parity with the United Kingdom and adopts the processes, regulations and laws in alignment as well as similar EU Regulations e.g. GDPR all of which support the compliance for domains.

NB: **The figure does not reflect the execution of any processes, laws or regulations**.



Italy

Commentary

Financial Regulatory Authority

https://www.bancaditalia.it/homepage/index.html (i)
https://www.ivass.it/homepage/index.html (ii)
https://www.consob.it/web/consob-and-its-activities/consob (iii)

The **Banca d'Italia** is the central bank of the Republic of Italy. It is a public-law institution regulated by national and European legislation and is an integral part of the **Eurosystem.**

The Bank of Italy operates under three dimensions: **international, national and local.**

The Bank is divided into branches which are situated in the regional capitals and some provincial capitals. The branches are responsible for carrying out various tasks, including:

1. Banking and financial supervision
2. Protection of customers of banking and financial intermediaries
3. Monetary circulation and the payment system
4. Economic analysis and statistical surveys at a local level. (i)

The Institute for the Supervision of Insurance (**IVASS**) is a body endowed with legal personality under public law whose goal is to ensure adequate protection of insured persons with a view to the sound and prudent management of insurance and reinsurance undertakings and their transparency and fairness towards customers. IVASS pursues the stability of the financial system and markets. (ii)

The Commissione Nazionale per le Società e la Borsa (**CONSOB)** is the government authority of Italy responsible for regulating the Italian financial markets. Their main aim is to protect investors and ensure '*efficiency, transparency and development of the market'* (iii)

The official currency in Italy is the **euro.**

AI Act / Policy

https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence (i)
https://www.agid.gov.it/sites/agid/files/2024-07/Italian_strategy_for_artificial_intelligence_2024-2026.pdf (ii)

As an EU Member State, Italy is bound by the **EU AI Act 2024.** (i)

The **Italian Strategy for Artificial Intelligence 2024-2026** provides a comprehensive overview for how Italy intends to align itself more closely with European legislation, whilst '*promoting the development of anthropocentric, reliable and sustainable solutions*."

The Strategy aims to pursue the following strategic macro-objectives:

1. Supporting the creation and adoption of AI applications, with a particular emphasis on developing systems from a country-specific perspective to preserve Italy's competitive differentials.
2. Promoting both foundational and applied AI research, integrating national units with international development platforms. This includes developing applications that are consistent with Italy's competitive needs whilst also supporting initiatives in relation to social welfare.
3. Create favourable conditions in the context of AI value generations, with a specific focus on growing talents and skills required to improve public services via AI solutions.

(ii)

Commentary

Anti-Money Laundering

https://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta=2007-12-14&atto.codiceRedazionale=007X0246&currentPage=1 (i)

https://www.bancaditalia.it/compiti/supervisione-normativa-antiriciclaggio/index.html?com.dotmarketing.htmlpage.language=1 (ii)

On a national level, Italy's anti-money laundering policies are enshrined within the **Legislative Decree 231/2007**. This outlines the duty of the Bank of Italy in regulating and supervising intermediaries for the purposes of combatting money laundering and the financing of terrorism (AML/CFT).

(i)

As a member of both the EU and the Financial Action Task Force (FATF), Italy transposes **EU laws and directives,** as well as the **FATF's 40 recommendations** into its AML/CFT legislation.

(ii)

Bribery

https://www.agenziacoesione.gov.it/wp-content/uploads/2023/01/italy-phase-4-report.pdf

The OECD Working Group on Bribery's phase 4 report evaluates Italy's implementation and enforcement of the **OECD's Anti-Bribery Convention.**

The Report found that Italy had successfully implemented a range of measures to combat bribery, including:

- Lengthening the statute of limitations for natural persons
- Increasing the number of imprisonment terms and disqualification sanctions
- Introducing whistleblower protection

Despite the Government's successes in tackling the bribery of individuals, the Working Group still identified concerns over Italy's legislation for holding companies accountable, indicating that the penalties were not fit for purpose.

Cloud Poli-cy

https://docs.italia.it/italia/cloud-italia/strategia-cloud-italia-docs/it/stabile/index.html

Digitisation of the Public Administration is one of the Italian Government's key priorities. Their mission is to ensure the 'quality, efficiency and effectiveness' of public services improves. As such, the **Cloud Strategy Italy** endeavours to achieve this goal by providing a strategic direction for implementing **cloud solutions in the Public Administration.**

The Strategy is formed on three foundational pillars:

1. Creating a National Strategic Hub (**PSN**), a national infrastructure for cloud service provision.
2. Introducing a **qualification process** for public cloud suppliers to ensure they meet the necessary security and reliability requirements and are compliant with relevant regulations.
3. Developing a **classification methodology** for data and services managed by public administrations.

https://en.agcm.it/en/scope-of-activity/consumer-protection/ (i)
https://www.mimit.gov.it/it/mercato-e-consumatori/tutela-del-consumatore/codice-del-consumo (ii)
https://ecc-netitalia.it/en/ (iii)

The powers of the Italian Competition Authority (**ICA**) have evolved over the years. They are now responsible for the following:

1. Repressing misleading advertising
2. Assessing comparative advertising
3. Impose fines on those who try to distort the economic choices of a consumer
4. Protect consumers against unfair commercial practices

(i)

The most consequential piece of legislation in Italy pertaining to consumer protection is the **Consumer Code (Legislative Decree 6 September 2005, n. 206).**

The Consumer Code performs various functions, including:

1. Consolidating the main provisions regarding consumer protection on a national level and those adopted in European legislation
2. Regulating relationships between consumers and professionals by stipulating their rights and obligations
3. Outlining protocols and procedures regarding out-of-court consumer disputes resolutions.

The Code also covers various phases of consumer relationships as depicted below.

(ii)

As an EU member, Italy has a designated European Consumer Centre (**ECC**). The Italian ECC acts as the national contact point for the **ECC Network**, which aims to enhance consumer trust in cross-border purchases.

Figure 22 Italian Consumer Code relationships.

(iii)

Commentary

Data / Privacy

https://www.garanteprivacy.it/web/garante-privacy-en (i)
https://www.garanteprivacy.it/web/garante-privacy-en/the-italian-data-protection-authority-who-we-are (ii)
https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9042678 (iii)

The Italian Data Protection Authority (**DPA**), otherwise known as the Garante, is an independent regulatory body, established pursuant to the privacy law (**Law No. 675 of 31 December 1996**) and regulated subsequently by the Personal Data Protection Code (**Legislative Decree No. 196 of 30 June 2003**) as amended by Legislative Decree No. 101 of 10 August 2018. (i)

This **DPA** is the supervisory authority responsible for monitoring the application of the EU's GDPR. Furthermore, they are committed to ensuring all data processing in the public and private sectors is compliant with relevant laws and that the rights of individuals are respected.

(ii)

The **Personal Data Protection Code** contains provisions for transposing EU law into national legislation.

(iii)

Fraud

https://www.adm.gov.it/portale/en/direzione-antifrode (i)
https://www.gazzettaufficiale.it/dettaglio/codici/codicePenale/438_1_1 (ii)

The **Anti-Fraud Directorate** operates within the Ministry of Economy and Finance and responsible for monitoring and analysing trade flows to formulae risk-profiles. Additionally, they ensure participation in anti-fraud working groups and committees on a national and international level, implementing strategies within the framework of the **Convention with the National Anti-Mafia and Anti-Terrorism Directorate.**

(i)

The various types of fraud and the penalties in place for those convicted are listed in **Chapter 2 of the Italian Criminal Code, Articles 640-645.**

(ii)

Sanctions

https://www.esteri.it/en/politica-estera-e-cooperazione-allo-sviluppo/politica_europea/misure_deroghe/

As a member of the EU, Italy is bound by the sanction lists and supports the **UN** sanctions.

In accordance with the framework of the Common Foreign Security Policy (**CFSP**), the EU applies restrictive measures for the purpose of achieving CFSP objectives.

Commentary

Terrorism

https://www.esteri.it/en/politica-estera-e-cooperazione-allo-sviluppo/temi_globali/lotta_terrorismo/ (i)

https://www.adm.gov.it/portale/en/adm-per-le-istituzioni-dello-stato#:~:text=The%20Antimafia%20and%20Anti%2Dterrorism,and%20monitors%20serious%20criminal%20investigations. (ii)

Italy has implemented a range of measures to combat terrorism. For instance, in 2015, they adopted **Law Decree No. 7,** pursuant to **UN Security Council Resolution No. 2178** of September 2014, aimed at addressing the phenomenon of so-called Foreign Terrorist Fighters (**FTF**).

Law 43/2015 also seeks to broaden the scope of existing counter-terrorism measures e.g. incriminating the 'recruit' as well as the 'recruiter'.

(i)

The Anti-Mafia and Anti-terrorism National Directorate (**DNA**) is the public body responsible for overseeing and monitoring serious criminal investigations in relation to mafia/terrorist related offenses.

(ii)

Company Registrar

https://italianbusinessregister.it/en/lists-of-companies (i)

https://italianbusinessregister.it/en/home (ii)

The Italian business register is where you can search and register companies.

(i)

The register also offers various other search functions e.g. company reports, annual accounts etc.

(ii)

Access to Public Information

https://www.protezionecivile.gov.it/en/department/transparent-administration/other-contents/civic-access/#:~:text=Simple%20civic%20access%20allows%20anyone,the%20institutional%20website%20of%20the

In accordance with Legislative Decree No. 97 of May 25, 2016, i.e. the **General Civic Access Law,** any Italian citizen has the right to access data and documents held by public administrations, providing they do not violate the 'protection of legally relevant interests.

Other

https://www.governo.it/en

Official Italian Government Presidency of the Council of Ministers website.

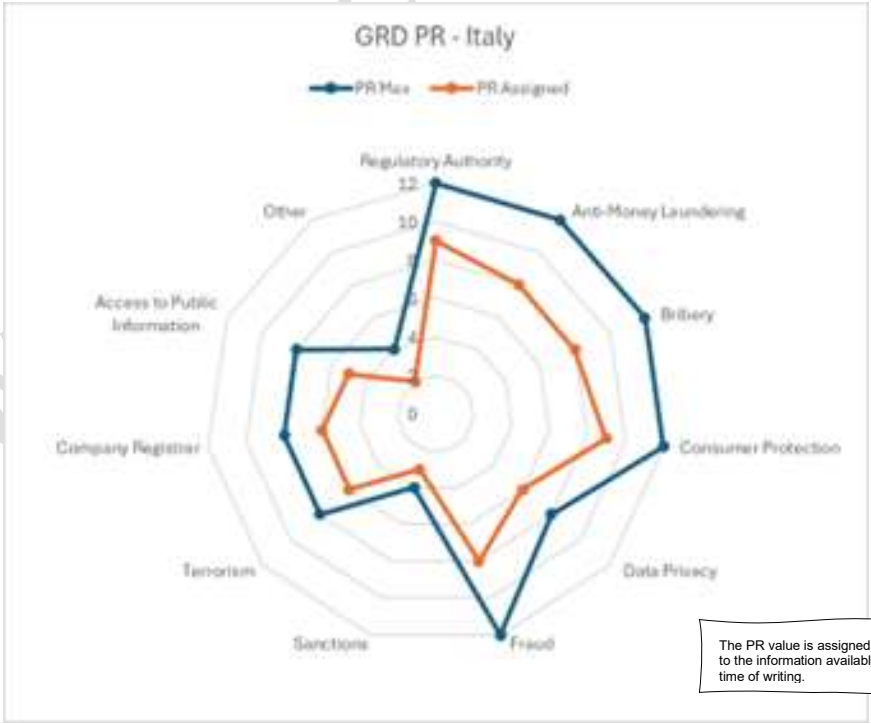
Posture Rating - Italy

The PR value of **7.0** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	9	8	8	9	6	8	3	6	6	5	2

Italy, as a member of the EU, has incorporated and expanded the regulations and laws to meet its obligations with the supporting processes.

NB: **The figure does not reflect the execution of laws and regulations for the domains**.



The PR value is assigned subject to the information available at the time of writing.

Japan

Commentary

Financial Regulatory Authority

https://www.boj.or.jp/en/ (i)
https://www.japaneselawtranslation.go.jp/en/laws/view/3788/en (ii)

The Bank of Japan is the central bank of Japan. The bank is often called Nichigin for short.

(i)

Governed by the **Bank of Japan Act**, the Bank's primary objective is to maintain price stability. This mandate is fulfilled through the issuance of banknotes and the implementation of monetary and currency controls.

The Bank of Japan operates independently from the Government. However, the Bank still maintains close collaboration to ensure their stance on monetary and currency controls are compatible with the Government's economic policies.

(ii)

The national currency in Japan is the Japanese **yen**.

AI Act / Policy

https://www8.cao.go.jp/cstp/ai/aistrategy2022_honbun.pdf (i)
https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20240419_9.pdf (ii) ~ **provisional translation**

Japan's **AI Strategy 2022** outlines a comprehensive framework for enhancing the implementation of AI in Japan. It acts as an extension of the former 2019 strategy, addressing a wider range of risk factors e.g. the pandemic. Furthermore, it outlines how AI can be utilised to resolve global issues, along with some of Japan's own social and economic problems.

The Strategy is formulated based on five key strategic objectives:

1. **Dealing with Imminent Crises** – Maximising protection of people and properties against large scale disasters e.g. pandemics
2. **Human Resources** – Developing a sustainable framework for attracting AI-centred human resources
3. **Technological Systems** – Establishing a framework for the implementation of technological systems
4. **Industrial Competitiveness** – Promoting AI adoption in real-world industries.
5. **International Cooperation** – Creating an international AI infrastructure in areas such as research and education

(i)

Japan advocates a concept named **'Society 5.0'**; a vision of a human-centric society that utilises a 'Cyber-Physical System' to foster economic growth and address social challenges. To realize this vision, Japan established the **'Social Principles of Human-Centric AI'** in 2019, guiding the responsible and ethical adoption of AI within society.

(ii)

Commentary

Anti-Money Laundering

https://www.mof.go.jp/english/policy/international_policy/amlcftcpf/3.efforts.html (i)
https://www.mof.go.jp/english/policy/international_policy/amlcftcpf/National_AML_CFT_CPF_Action_Plan_FY2024-26.pdf (ii)

The four pillars of the **AML/CFT/CPF regime** in Japan are:

1. Preventative measures by financial institutions and designated non-financial. businesses and professions.
2. Criminalising Money Laundering and Terrorism Financing
3. Depriving criminal proceeds.
4. Combatting the financing of terrorism and countering proliferation financing.

Considering the FATF's Fourth Round of Mutual Evaluation Report, the Government of Japan established the **Interministerial Council for AML/CFT/CPF Policy.** This is co-chaired by the National Police Agency (**NPA**) and the Ministry of Finance (**MOF**), with the purpose of developing, coordinating and promoting national AML/CFT/CPF policies.

(i)

The **National AML/CFT/CPF Action Plan** outlines a range of anti-money laundering measures scheduled to take place between 2024-2025, clearly stipulating intended outcomes and the authorities in charge of their implementation.

(ii)

Bribery

https://www.jica.go.jp/Resource/english/our_work/compliance/c8h0vm00009ulm1i-att/anti_corruption_guidance_en.pdf (i)
https://www.oecd.org/en/topics/sub-issues/fighting-foreign-bribery/japan-country-monitoring.html (ii)

In 2014, the Japan International Cooperation Agency (**JICA**) issued a comprehensive policy document instructing all entities involved in Official Development Assistance (**ODA**) to implement measures aimed at preventing and combating bribery and corruption within their operations.

(i)

Japan is party to the **OECD Anti-Bribery Convention**. As such, it is subject to rigorous peer-review and monitoring by the OECD Working Group on Bribery regarding its implementation of anti-bribery and corruption measures.

(ii)

https://www.caa.go.jp/en/about_us/ (i)
https://www.cao.go.jp/consumer/en/e-index.html (ii)
https://www.kokusen.go.jp/e-hello/about_ncac/data/ncac_hello.html (iii)
https://www.japaneselawtranslation.go.jp/en/laws/view/3578/en#:~:text=Article%201The%20purpose%20of,and%20quantity%20of%20information%20and (iv)

The Consumer Affairs Agency of Japan (**CAA**) is headed by the Minister of State for Consumer Affairs and Food Safety, under the authority of the Prime Minister.

The CAA's main purpose is to protect and promote consumer rights. They achieve this by shaping consumer policy and ensuring government members take appropriate actions to prevent deceptive and unfair business practices.

(i)

The **Consumer Commission** was first established in 2009 as an independent third-party organization, conducting investigations and deliberations for the Consumer Affairs Agency and other relevant government agencies.

(ii)

The National Consumer Affairs Centre of Japan (**NCAC**) was introduced in 1970. They engage in various activities pertaining to consumer protection, including:

- Supporting consumer consultation services
- Carrying out Alternative Dispute Resolution (ADR)
- Conducting research on consumer affairs and sharing information via various platforms

(iii)

The **Consumer Contract Act 2000** is a crucial piece of legislation with regards to consumer protection in Japan. The purpose of the Act is to protect the interest of consumers, contributing to the overall welfare of Japanese citizens and the health of the national economy.

The Act covers multiple areas, as depicted below:

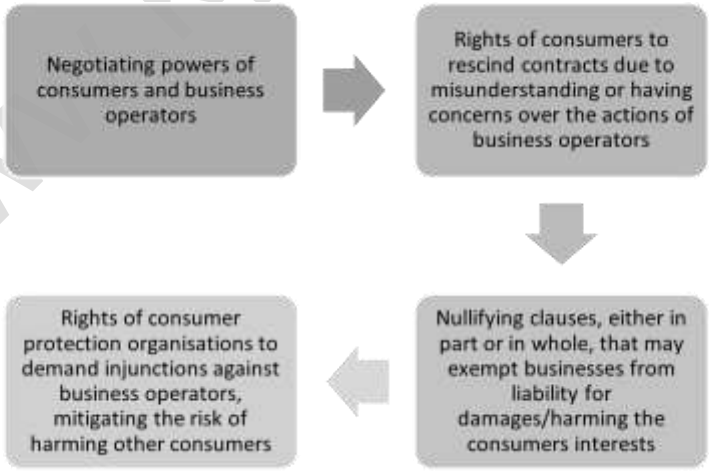


Figure 23 Japan - Consumer Contract Act 2000

(iv)

Commentary

Cloud Policy

https://www.meti.go.jp/english/press/2024/0419_001.html#:~:text=In%20light%20of%20this%20situation,computational%20resources%20in%20Japan%20for (i)

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/bc5a569f-71d0-44d9-b5c9-cc9b59405507/47b4badd/20231228_en_priority_summary_01.pdf (ii)

The Ministry of Economy, Trade and Industry (**METI**) approved plans for ensuring a stable supply of cloud programmes under the **Economic Security Promotion Act.** The main motivation behind this is to strengthen Japan's cloud service provision, ensuring it does not rely too heavily on services provided by foreign companies.

(i)

In 2023, Japan's **Digital Agency** unveiled the **Priority Policy Programme for Realising Digital Society**. Cloud solutions are central to the Government's vision of a Digital Society. A key aspect of this vision is the ***'cloud by default principle***,' which mandates that cloud solutions be the preferred choice for developing information systems within all ministries, including those related to cyber security.

(ii)

Data / Privacy

https://www.ppc.go.jp/en/aboutus/commission/ (i)

https://www.ppc.go.jp/en/aboutus/roles/ (ii)

https://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf (iii)

The Personal Information Protection Commission (**PPC**) is comprised of eight Commission members, appointed by the Prime Minister with the consent of both Houses of the Diet.

(i)

The main purpose if the PPC is to protect the rights and interests of individuals whilst supervising the appropriate use of personal information.

The PPC operates independently and is governed by the **Protection of Personal Information Act.**

(ii)

The **Act on the Protection of Personal Information, 2003** is the most consequential piece of legislation in Japan regarding data privacy. The primary aim of the Act is to protect individuals' data privacy rights, whilst also promoting the utilization of personal information to advance information and communications in society. It strives to achieve this by:

1. Clearly stipulating the duties and responsibilities of the State and local governments
2. Establishing a basic framework for the Government to implement regarding data protection
3. Outlining the duties of data processors and handlers

(iii)

Commentary

Fraud

https://www.cas.go.jp/jp/seisaku/hourei/data/PC.pdf (i)
https://www.jica.go.jp/english/about/basic/oda/index.html (ii)
https://www.contact.mofa.go.jp/form/pub/mofaj-oda/fusei_en (iii)

Fraud is criminalised in Japan, as stipulated in the **Penal Code (Act No.45 of 1907)** under the following articles: (i)

Article 246 – General Fraud → **Article 246.2 – Computer Fraud** → **Article 248 – Quasi Fraud**

Japan participates in delivering Official Development Assistance (**ODA**), i.e. providing financial support to developing countries with the aim of boosting their social and economic landscape.

Japan's International Cooperation Agency (**JICA**) and the Ministry of Foreign Affairs (**MOFA**) both play a key role in delivering Japan's ODA objectives. This also involves closely monitoring activities to ensure no fraudulent or corrupt practices are taking place.

Both the JICA and MOFA provide an **ODA consultation desk**, designed to provide information to concerned entities regarding fraud and corruption in Japan's ODA projects. (ii)/(iii)

Sanctions

https://www.mof.go.jp/policy/international_policy/gaitame_kawase/gaitame/economic_sanctions/list.html

Ministry of Finance Economic Sanctions and List of Affected Persons – **Japanese with some English Elements.**

Terrorism

https://www.mofa.go.jp/region/n-america/us/terro0109/policy/index.html (i)
https://japan.kantei.go.jp/policy/2001/anti-terrorism/1029terohougaiyou_e.html (ii)

The Ministry of Foreign Affairs (**MOFA)** is the government body primarily responsible for combatting terrorism in Japan. A full list of their polices and measures is available on their official website. (i)

One of the most significant pieces of legislation regarding countering terrorism in Japan is the **Anti-Terrorism Special Measures Law.**

The main purpose of the Act to implement the **UN Security Council's Resolution's** on international terrorism, ensuring Japan can effectively contribute to the international community and strive towards peace and security, both on a national level and international level. (ii)

Company Registrar

https://www.moj.go.jp/EN/MINJI/houjintouki.html (i)
https://www2.jpx.co.jp/tseHpFront/JJK020010Action.do?Show=Show (ii)

Companies in Japan can be registered via the Ministry of Justice website. (i)
Japan's company registrar can be searched via the Japan Exchange Group website. (ii)

Access to Public Information

https://www.soumu.go.jp/english/gyoukan/engv1_03.pdf

The Act on **Access to Information Held by Administrative Organs (Act No. 42 of 1999)** provides Japanese citizens the right to request access to public documents held by administrative bodies i.e. any entity within the Cabinet or under the jurisdiction of the Cabinet.

Other

https://www.japan.go.jp/

The official website of the Government of Japan.

Posture Rating – Japan

The PR value of **7.8** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigne	10	9	9	10	7	10	3	6	6	5	3

Japan has well defined processes, regulations and laws to address the various domain and support its international obligations.

Although Japan scores well across all domains it should be noted that many of the documents relating to regulations were not available in English and the PR value reflects this.

NB: **The figure does not reflect the execution of these laws and regulations**.

Jersey

Commentary

Financial Regulatory Authority

https://www.jerseyfsc.org/ (i)
https://www.jerseylaw.je/laws/current/l_11_1998 (ii)

The Jersey Financial Services Commission is the regulator of financial services in the Channel Island of Jersey. (i)

The JFSC is governed by the **Financial Services Commission (Jersey) Law 1998**. This sets out the Commission's statutory responsibilities, including:

1. Authorizing, supervising, monitoring and developing financial services in Jersey
2. Ensuring compliance with the Commission Law
3. Reporting, advising, assisting and informing the Government of Jersey and other relevant state authorities on financial regulatory issues
4. Developing financial policies and regulations
5. Operating the Company Registrar

(ii)

Jersey is in currency union with the United Kingdom and as such the **Jersey pound** maintains the same currency value as the British pound.

AI Act / Policy

https://www.digital.je/our-work/5-year-strategy/ (i)
https://www.gov.je/SiteCollectionDocuments/Education/P%20AI%20In%20Jersey%20Education%20Policy%2020231006.pdf (ii)

Digital Jersey's - 5 Year Strategic Plan identified some significant gaps in Jersey's digital adoption compared to its UK counterparts, which the Government feels is stifling their overall business productivity. Believing this, the Government set an ambitious target of improving the sectoral adoption of new technologies, such as AI, by 150% over the next 5 years.

To achieve this target, the Government have already been implementing several measures, including:

1. Driving the adoption of new technologies and the recruitment of digital skills
2. Delivering **Sector-by-Sector Technology Roadmaps** to support the digital transformation of Jersey's key industries
3. Targeted **digital competencies training** targeted towards non-digital small and medium enterprises (SMEs) (i)

The Government of Jersey has emphasised their commitment to improving digital adoption across key industries. One prime example is the **AI Policy – Generative AI in Jersey Education** publication, issued by the Government of Jersey Children Young People Education and Skills (**CYPES**) Department.

Within this policy document, the CYPES explore the potential of AI, including generative AI, as a force for good in the education sector. They set out a comprehensive ethical framework for how AI could be adopted responsibly, highlighting some of the following objectives:

- Using AI to alleviate teacher's workload and enhance organization capabilities, whilst still respecting the value of human relationships
- Using AI to evaluate and acknowledge a wider spectrum of learners (ii)

Commentary

Anti-Money Laundering

https://www.jerseylaw.je/laws/current/l_8_1999 (i)
https://www.jerseyfsc.org/industry/financial-crime/amlcftcpf-legislation/ (ii)

The most consequential piece of legislation pertaining to money laundering in Jersey is the **Proceeds of Crime (Jersey) Law 1999**.

The Law covers a range of topics, including:

1. Confiscation orders and instrumental forfeiture orders i.e. depriving offenders of their proceeds of criminal conduct
2. Procedures to prevent and detect money laundering
3. Obligations of financial institutions to report suspicious activities to the Financial Intelligence Unit (FIU) or designated officer
4. External confiscation orders

(i)

Another key law in relation to money-laundering is the **Proceeds of Crime (Supervisory Bodies) (Jersey) Law 2008**.

The Law stipulates that the **JFSC** is the leading supervisory body responsible for ensuring compliance with AML/CFT regulations in Jersey. Additionally, it states that the Minister may appoint **additional bodies** to perform supervisory functions, providing they meet eligibility requirements.

The Law also covers:

1. Powers and duties of supervisory bodies, including the requirement to adopt a risk-based approach
2. The company registration process
3. Rights of supervisory bodies to obtain information and investigate offences

Full list of Jersey's AML/CFT/CPF legislation can be accessed via the **JFSC website**.

(ii)

Bribery

https://www.jerseylaw.je/laws/current/PDFs/L_12_2006.pdf

The customary law offence of bribery was abolished and replaced with the Corruption (Jersey) Law 2006 (14th April 2025).

Jersey's Anti-Corruption Policy aims to establish a '*zero-tolerance*' approach towards any form of corruption in Jersey.

The policy outlines some key principles which the State abides by in relation to preventing bribery and corruption. These include:

1. Fair, open and honest business activities
2. Avoiding business relationships with entities that do not uphold strict anti-bribery and anti-corruption standards
3. Carrying out risk-assessments and due diligence measures, including drawing up suitable anti-bribery and corruption clauses within contracts

Commentary

Consumer Protection

https://www.gov.je/Industry/RegulatingUnfairCommercialPractices/pages/unfaircommercialpracticeslaw.aspx (i)
https://www.jerseylaw.je/laws/enacted/Pages/L-16-2018.aspx (ii)

The **Consumer Protection (Unfair Practices) (Jersey) Law, 2018** is designed to protect both consumers and businesses.

The Law bans traders across all industries from using unfair commercial practices e.g. preventing sellers from using aggressive sales tactics or misleading consumers about products and or services.

(i)

The full version of the law can be accessed via the **Jersey Legal Information Board's official website**. The main areas covered in the Law are as follows:

1. Defining what constitutes an unfair practice i.e. any practice that causes harm or is likely to cause harm to the economic interests of the average consumer
2. Implementing penalties for those in violation of consumer protection law
3. Stipulating the powers of authorized officers to investigate and undertake actions to prevent such practices

(ii)

Cloud Policy

https://www.digital.je/our-work/5-year-strategy/ (i)
https://www.digital.je/news-events/digital-news/events-will-demystify-the-cloud-for-channel-island-businesses/ (ii)

Digital Jersey's 5-Year Strategic Plan prioritises investing in the digital economy to foster sustainable, long-term growth. A key element of this strategy is ensuring the Government fully leverages cloud computing and other technological infrastructures.

(i)

The Government has already made big commitments to increasing public spending on digital economy initiatives. For example, investing in the **Island Infrastructure Fund** and directing funds to key digital economy infrastructure and institutions e.g. **Digital Jersey.**

(ii)

Data / Privacy

URL

https://www.jerseylaw.je/laws/current/PDFs/L_3_2018.pdf (i)
https://www.gov.je/Government/dataprotection/pages/dataprotectioninjersey.aspx (ii)
https://www.jerseylaw.je/laws/enacted/Pages/L-04-2018.aspx (iii)
https://www.jerseyoic.org/about-joic/ (iv)

The **Data Protection (Jersey) Law 2018** is one of the most significant pieces of legislation in Jersey pertaining to consumer protection.

(i)

Figure 24 Jersey Data Protection Law 2018 Components

Whilst Jersey is not bound by Europe's **GDPR**, the Data Protection Law of 2018 introduced equivalent principles, strengthening Jersey's overall privacy rights.

(ii)

Data Protection Authority (Jersey) Law 2018 was issued with the purpose of introducing a new statutory body in Jersey to oversee the protection of personal data.

As stipulated in the Law, the Data Protection Authority must appoint an **Information Commissioner**, acting as the Chief Executive of the Authority.

(iii)

The Jersey Office of the Information Commissioner (**JOIC**) sits within the Jersey Data Protection Authority. The JOIC is an independent regulatory body, responsible for overseeing the **Data Protection Law of 2018** and the **Freedom of Information Law of 2011.**

(iv)

Commentary

Fraud

https://www.jerseyauditoffice.je/wp-content/uploads/2021/01/Anti-Corruption-Arrangements-report-27.01.2021.pdf (i)

https://www.jerseylaw.je/laws/current/I_14_1967 (ii)

https://www.fraudprevention.je/ (iii)

Jersey's Audit Office issued an insightful review into the Island's anti-fraud and corruption measures, including the **Counter Fraud and Corruption Strategy.**

The review emphasized the need for stronger counter-fraud measures in Jersey. The Government has already begun to address this by separating fraud and corruption in the new Anti-Corruption Policies, enabling a more targeted approach.

Additionally, in response to the Covid-19 Pandemic, three departmental risk-registers were updated to include specific references to fraud and corruption. These are as follows:

1. **Treasury and Exchequer** – Risks associated with financial measures to support Covid-19 processes.
2. **Customer and Local Services** – Fraud in relation to claim schemes.
3. **Chief Operating Office** – Commercial fraud linked to increased activity and unsupervised staff working from home.

(i)

The **Investors (Prevention of Fraud) (Jersey) Law, 1967** legislates against fraudulent inducements to invest money i.e. intentionally deceiving someone with the aim of persuading them to enter into a contract or agreement.

(ii)

The **Jersey Fraud Prevention Forum** website is the designated platform for citizens to report fraudulent scams.

(iii)

Sanctions

https://www.gov.je/Government/Departments/JerseyWorld/pages/sanctionsfaq.aspx#:~:text=In%20addition%20to%20UNSC%20sanctions,sanctions%20and%20autonomous%20UK%20sanctions.

Jersey implements sanctions made by the United Nations Security Council (**UNSC**) and the **UK's** own autonomous sanctions.

The Sanctions and Asset-Freezing (Jersey) Law 2019 (**SAFL**), along with the **External Sanctions Order 2021**, ensures that the Island of Jersey can implement UNSC and autonomous UK sanctions in a timely manner and in line with international standards.

Commentary

Terrorism

https://www.gov.je/Government/Departments/JerseyWorld/pages/measuresagainstterrorism.aspx (i)
https://www.jerseylaw.je/laws/current/I_40_2002 (ii)
https://www.gov.uk/government/publications/proscribed-terror-groups-or-organisations--2 (iii)

The Sanctions and Asset-Freezing (Jersey) Law 2019 (**SAFL**) is one of the most consequential pieces of legislation in Jersey pertaining to combatting terrorism and terrorist financing.

In accordance with the SAFL, any person or entity believed to be involved in or supporting terrorist activities must be prohibited from accessing all funds, financial services and economic resources.

(i)

Another crucial piece of legislation is the **Terrorism (Jersey) Law 2002.** This covers a range of topics, including:

1. Proscribed organizations i.e. how they are listed, processes for de-listing etc.
2. Offences related to terrorist financing
3. Terrorist investigations and counter-terrorist powers e.g. rights for the police to stop and search
4. Further terrorist offences e.g. weapons training, inciting terrorism overseas (ii)

As a **British Crown Dependency**, Jersey adopts the **UK's list** of proscribed terrorist groups and organizations within its anti-terrorism legislation.

(iii)

Company Registrar

https://www.jerseyfsc.org/registry/ (i)
https://www.jerseyfsc.org/#search_regulated (ii)

The Jersey financial services commission is where to search the registers. (i)
The Jersey search capability of regulated businesses. (ii)

Access to Public Information

https://www.gov.je/Government/FreedomOfInformation/pages/index.aspx (i)
https://www.gov.je/Government/FreedomOfInformation/Pages/PublishedInformation.aspx (ii)
https://www.gov.je/Government/FreedomOfInformation/Pages/MakeFOIRequest.aspx (iii)

Jersey's **Freedom of Information (FOI) Law, 2011** provides the citizens of Jersey access to information held by public bodies.

(i)

A large amount of public information is readily available via the Government website.

(ii)

If the information is not already available, one can make a **FOI request** via the Government website (*onegov account required*).

(iii)

Other

https://www.gov.je/pages/default.aspx

The official information and public services for the Island of Jersey.

Posture Rating- Jersey

The above PR value of **7.0** rating is derived using the following assigned values.

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assign	7	7	8	8	7	9	3	6	7	6	2

As a British Crown Dependency, Jersey has adopted and adapted best practice both from the UK and the European Union to provide the processes, regulations and laws to support the domains.

Jersey benefits from size when interacting with its citizens and this is reflected in the access to information assigned value.

NB: **The figure does not reflect the execution of any laws and regulations**.

The Hashemite Kingdom of Jordan

Commentary

Financial Regulatory Authority

https://www.cbj.gov.jo/EN/Pages/Welcoming_Note (i)
https://jsc.gov.jo/page/en/strategic_objectives (ii)

The Central Bank of Jordan (**CJB**) was first established as a monetary authority in 1964, operating as an **independent and autonomous** corporate identity.

The main functions of the CJB include:

1. Maintaining monetary and financial stability
2. Serving as a Banker for smaller banks, specialised lending institutions, the government and official public bodies
3. Implementing measures to solve financial and economic problems,
4. Advising the government on financial and economic policy
5. Setting out rules and disciplines for banks to follow regarding customer relations

(i)

Jordan's Security Commission (JSC) is another key authority, responsible for regulating, monitoring and developing Jordan's capital markets.

The Commission's regulatory activities are underpinned by **three key objectives:**

1. Regulating and developing the capital market
2. Protecting the Amman Stock Exchange (ASE) investors and securities
3. Protecting the capital market from potential risks

(ii)

The Jordanian **dinar** is the official currency of Jordan.

AI Act / Policy

https://www.modee.gov.jo/ebv4.0/root_storage/en/eb_list_page/40435648.pdf

Jordan's Artificial Intelligence Strategy and Implementation Plan outlines a 5-year roadmap, building upon the foundation of previous government-led digital transformation initiatives.

The Strategy is founded on **five key objectives:**

1. Building capacity and upskilling Jordanian workforce
2. Promoting scientific research and development
3. Improving the environment for investment and entrepreneurship in the field of AI
4. Ensuring legislation and regulations support the safe use of AI
5. Utilising AI tools to drive efficiencies in public and priority sectors.

Commentary

Anti-Money Laundering

https://www.amlu.gov.jo/Default/Ar (i)

https://www.amlu.gov.jo/ebv4.0/root_storage/en/eb_list_page/anti_money_laundering_and_counter_terrorist_financing__law_no._(20)_of_2021.pdf (***unofficial English translation***) (ii)

The Anti-Money Laundering and Terrorist Financing Unit (AMLU) of Jordan was established in accordance with Law No. (46) of 2007, Anti-Money Laundering and Combatting the Financing of Terrorism.

The AMLU is a government agency with **financial and administrative independence**. Some of the main duties and responsibilities of the Unit include:

- **Investigating and analysing** notifications/reports concerning AML/CFT crimes to help inform competent authorities
- **Implementing policies** of the National Committee for Combatting AML/CFT.

(i)

The **Anti-Money Laundering and Counter Terrorist Financing Law 2021** replaced the original 2007 legislation, seeking to provide Jordan with a more robust AML/CFT. framework.

Some of the main features of the Law are as follows:

1. Outlining obligations of financial institutions to establish AML policies and procedures
2. Requirements for financial institutions and other supervised entities to implement customer due diligence measures, report suspicious transactions and maintain accurate records
3. Penalties for non-compliance, including fines, sanctions or criminal charges

(ii)

Bribery

https://www.jiacc.gov.jo/EBV4.0/Root_Storage/AR/EB_Blog/JIACC_Strategy_2020-2025_English.pdf

---

The **National Integrity and Anti-Corruption Strategy 2020-2025** is Jordan's five-year plan for enhancing law enforcement and preventative measures for combatting bribery and corruption.

The strategy is composed of 24 projects, all of which target one of the following areas:

1. Promoting integrity and corruption prevention
2. The rule of law
3. Building organizational capabilities

Project No. (6) focuses on developing proactive monitoring and investigative mechanisms. This includes field monitoring the practices of favouritism and bribery.

Commentary

Consumer Protection

https://www.mit.gov.jo/En/Pages/About_the_Ministry (i)
https://www.cbj.gov.jo/EN/List/Financial_consumer_protection (ii)
http://www.civilsociety-jo.net/en/organization/501/the-national-society-of-consumer-protection (iii)

Although Jordan lacks a specific government department for consumer protection, the **Ministry of Trade and Industry** assumes a pivotal role. A key national objective for the ministry is to strengthen consumer protection policies and guarantee the availability of high-quality goods in the market at fair prices.

The **Central Bank of Jordan (CJB)** is the main authority responsible for protecting the rights of consumers of financial services.

(i)

The CBJ have implemented various measures concerning consumer protection, including:

1. **Issuing instructions for licenced entitie**s on 'dealing with customers fairly and transparently'. This includes credit control requirements of retail portfolios and the need to establish complaint-handling units
2. **Amending the CBJ Law** to expand the scope of its functions
3. Establishing a **Financial Consumer Protection department** within the CBJ, responsible for setting rules and standards for licenced entities and raising public awareness of banking and other financial institution activities

(ii)

Cloud Policy

https://www.modee.gov.jo/ebv4.0/root_storage/en/eb_list_page/cloudpolicy-2020-english.pdf - ***unofficial English translation***

The Ministry of Digital Economy and Entrepreneurship issued Jordan's **Cloud (Platforms and Services) Policy 2020.**

The core objective of this policy is to foster the growth of Jordan's digital economy by establishing integrated cloud ecosystems for the Jordanian Cloud. To achieve this goal, the policy set various objectives, including:

- Encouraging government bodies to optimise cloud services
- Continuing the development of the government private cloud

Ensuring the protection of cloud service users through establishing a comprehensive regulatory framework.

Data / Privacy

https://www.modee.gov.jo/ebv4.0/root_storage/en/eb_list_page/pdpl.pdf (i)
https://www.modee.gov.jo/EN/Pages/Who_we_are_persona l (ii)

Personal Data Protection Law No. 24 of 2023 is the most significant piece of data protection legislation in Jordan.

The **scope of the Law** is vast, applying to all types of data (including data processed prior to the enactment of the Law). It does not however, apply to individuals processing their own personal data.

The Law covers various areas, including:

1. **Rights of data subjects** e.g. the right to withdraw consent and to object to the processing and profiling of data if it does not align with initial purpose of collection
2. Obligations of Data Controllers. This includes the requirement to appoint a **Data Protection Officer (DPO**) under certain conditions, e.g. if the primary activity of the controller is processing personal data
3. Establishing the **Personal Data Protection** (**PDP**) **Council**.

The PDP Council is chaired by the Minister of Digital Economy and Entrepreneurship and is comprised of several members other members, including the **Information Commissioner** (the vice-chair) and a representative from the CBJ**.** The Council performs various functions, including:

1. Approving policies, strategies and plans pertaining to data protection
2. Issuing licences and permits for storage, processing, profiling and transferring of data
3. Reviewing requests

(i)

The **Data Protection Unit (DPU)** is governed by the PDP Council and operates under the **Ministry of Digital Economy and Entrepreneurship**. One of the primary objectives of the Unit is to strengthen Jordan's data protection regulations and align them more closely with international standards.

The Unit is responsible for:

1. **Handling** personal information
2. **Investigating** reports and complaints
3. **Monitoring** compliance

(ii)

Fraud

https://amlu.gov.jo/ebv4.0/root_storage/en/eb_list_page/03_law_no._(18)_of_2017_securities_law-0.pdf (i)
https://www.cbj.gov.jo/ebv4.0/root_storage/en/eb_list_page/guidelines_on_combating_financial_fraud_within_the_national_payment_system-0.pdf (ii)

There is no standalone Law governing fraud in Jordan. That said, there are several industry-specific laws that criminalise fraudulent activities. For example, **Law No.(18) of 2017 Securities Law** ascertains that any licenced person who sells or disposes of securities without official authorisation is deemed to have committed fraud/forgery.

The CBJ issued a guidance document on Combatting Financial Fraud in the National Payment System. This is directed at companies licenced by the central bank, including banks and exchange companies. (i)

The guidance aligns with existing fraud legislation, serving as a useful tool for establishing robust governance practices for combatting fraud and ensuring companies can manage electronic payment systems effectively and efficiently. (ii)

Commentary

Sanctions

https://www.unodc.org/unodc/en/terrorism/latest-news/2024_unodc_-unodc-supports-jordan-to-implement-un-security-council-sanctions.html

Jordan does not have its own autonomous sanctions list. However, it does implement UN Security Council Sanctions.

Terrorism

https://www.amlu.gov.jo/ebv4.0/root_storage/en/eb_list_page/01_law_no.(20)_of_2021_-_anti_money_laundering_and_counter_terrorist_financing_law.pdf
(**unofficial translation**)

Law No.(20) of 2021 - Anti Money Laundering and Counter Terrorist Financing Law sets out various measures in relation to preventing terrorism. For instance, it stipulates that the Council of Ministers may establish one or more technical committees, specifically for the purpose of implementing the UN Security Council Resolutions pertaining to terrorism, terrorist financing and the financing of proliferation.

Company Registrar

https://ccd.gov.jo/Default/Ar (i)

https://portal.jordan.gov.jo/wps/portal/Home/GovernmentEntities/Agencies/AgencyServiceDetails_en/jordan+free+and+development+zones+group/services/issuance+of+a+certificate+of+company+registration?lang=en&content_id=com.ibm.workplace.wcm.api.WCM_Content/Issuance (ii)

Businesses can be registered via the Companies Control Department website. (i)

The official site of the Jordanian Government and where to search the company registration. (ii)

Access to Public Information

https://jsc.gov.jo/page.aspx?page_key=key_get_info&keywords=3&lang=en

In 2007, Jordan became the first Arab country to enact a freedom of information law, guaranteeing Jordanian citizens the **right to access information** held by public authorities, in line with international best practices.

Citizens can request information on the Securities Commission via their official website.

Other

https://form.jordan.gov.jo/wps/portal/Home

The official site for the Jordanian e-Government.

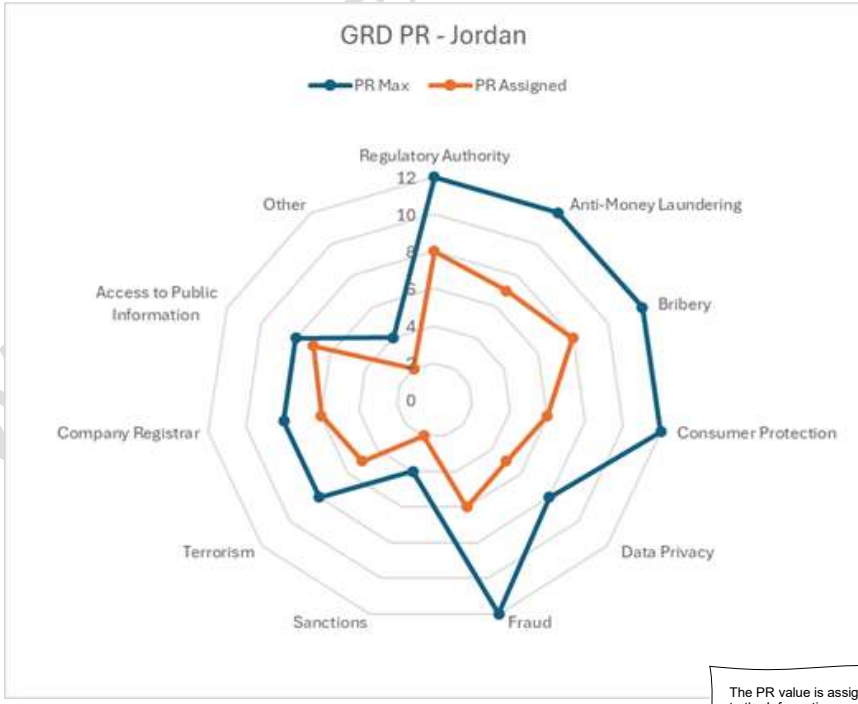
Posture Rating - Jordan

The PR value of **6.2** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	8	7	8	6	5	6	2	5	6	7	2

Jordan has defined processes, regulations and laws to meet domain obligations. However, in many cases there is no single law relating to a domain and dispersed across other laws which is factored into the PR score.

NB: **The figure does not reflect the execution of any laws and regulations**.



The PR value is assigned subject to the Information available at the time of writing.

Commentary

https://www.centralbank.go.ke/ (i)
https://www.centralbank.go.ke/wp-content/uploads/2016/08/CBKAct1stOct2015.pdf (ii)
https://www.cma.or.ke/about-us/ (iii)

The **Central Bank of Kenya (CBK)** is Kenya's main financial regulatory authority, established pursuant to Article 231 of the Constitution of Kenya. The main responsibilities of the Bank include formulating monetary policy; achieving and maintaining price stability; issuing currency which are provisioned through six core functions as depicted below:

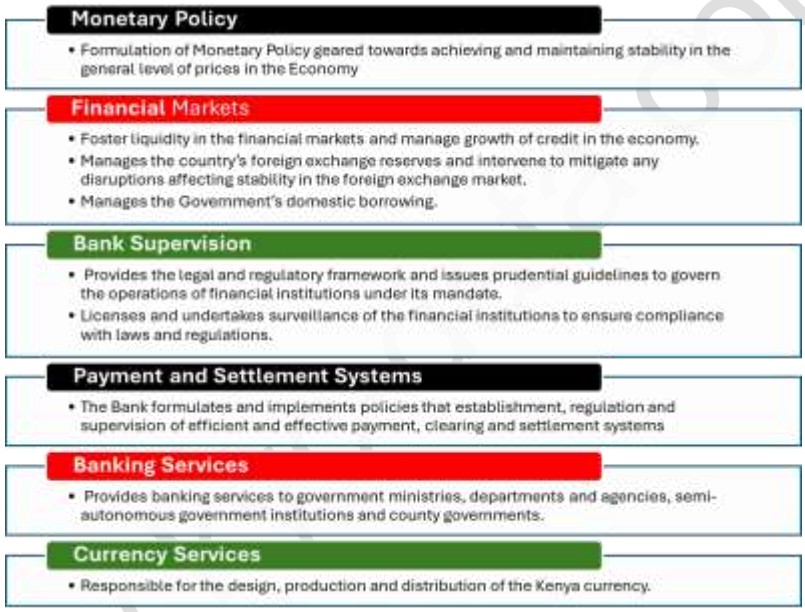


Figure 25 The Central Bank of Kenya's 6 core functions

(i)

In accordance with the CBK Act, the Bank promotes financial stability through various means, including:

1. Regulating, supervising and licencing financial institutions under its jurisdiction
2. Providing oversight of payment, clearing and settlement systems
3. Formulating and implementing foreign exchange policy and managing foreign exchange reserves
4. Acting as a banker, fiscal agent and advisor to the Government

(ii)

The **Capital Markets Authority (CMA)** is an independent public body, accountable for supervising, licencing and monitoring the activities of market intermediaries such as the **Stock Exchange** and the **Central Depository and Settlement Corporation**.

The CMA is also responsible for regulating all licenced entities under the Capital Markets Act. This includes online Forex, Commodities and Regulated Exchanges.

(iii)

Commentary

AI Act / Policy

https://ict.go.ke/sites/default/files/2024-09/MICDE%20Strategic%20Plan%202023-2027_0.pdf

Kenya's Ministry of Information, Communications and the Digital Economy (**MICDE**) issued Kenya's **Digital Strategy, 2023-2027**.

The overarching goal of this strategy is to shape policy for digital infrastructure and communications. This will be achieved by utilising technology and innovation to support socio-economic development and increase global competitiveness. This includes leveraging emerging technologies such as AI to improve efficiency and productivity.

Anti-Money Laundering

https://www.frc.go.ke/?page_id=7 (i)

https://new.kenyalaw.org/akn/ke/act/2009/9/eng@2022-12-31 (ii)

The Financial Reporting Centre (**FRC**) is Kenya's Financial Intelligence Unit, established pursuant to section 21 of the Proceeds of Crime and Anti-Money Laundering Act, 2009 (**POCAMLA**).

The FRC is operates as an independent body, serving to promote the integrity of Kenya's financial system through combating money laundering, the financing of terrorism and proliferation financing.

(i)

The **Proceeds of Crime and Anti-Money Laundering Act 2009** is arguably the most consequential piece of AML legislation in Kenya. The Act introduces various measures for combatting ML offences, making provisions for the *identification, tracing, freezing, seizure and confiscation* of the proceeds of crime.

In addition to the FRC, the Act also establishes the Anti-Money Laundering **Advisory Board**. Some of the main functions of the board are as follows:

1. **Advise the Cabinet Secretary** on policies, best practices and other related activities pertaining to combatting money laundering
2. **Advise the FRC** on its functions
3. Act as a **forum for the FRC**, state organs and other supervisory bodies, offering them a space to consult anti-money laundering developments, concerns and initiatives

(ii)

Commentary

Bribery

https://new.kenyalaw.org/akn/ke/act/2016/47/eng@2023-12-11 (i)
https://eacc.go.ke/en/default/about-us/ (ii)

The **Anti-Bribery Act 2017** was introduced by the Government of Kenya for the purpose preventing, investigating and punishing bribery.

The Act covers the following areas:

1. General **bribery offences** i.e. giving or receiving a bribe and bribery of foreign public officials
2. **Procedures** for the prevention of bribery e.g. bribery by a private entity and guidance for private entities in preventing bribery
3. **Other** provisions on offences e.g. obligations of public and private entities to report to the **Ethics and Anti-Corruption Commission** within 24 hours
4. **Penalties** for those in violation of anti-bribery law

(i)

The **Ethics and Anti-Corruption Commission** is responsible for enforcing the Anti-Bribery Act. They are mandated to combat and prevent corruption in Kenya through law enforcement, prevention and educating the public.

Reports of corruption taking place within Government and the public sector can be made directly to the Commission via their website.

(ii)

Consumer Protection

https://cak.go.ke/ (i)
https://new.kenyalaw.org/akn/ke/act/2012/46/eng@2022-12-31 (ii)

The Consumer Department of the **Competition Authority of Kenya (CAK)** has the primary function of investigating complaints pertaining to false or misleading representations, unfair business practices and the supply of unsafe, defective or unsuitable goods.

(i)

The **Consumer Protection Act 2012** makes provisions for the protection of consumers and preventing unfair trading practices occurring in consumer transactions.

The Act serves many purposes, including:

1. To **establish a legal framework** for achieving and maintaining a fair consumer market
2. Promoting **fair and ethical business practices**
3. Providing a 'consistent, accessible and efficient' system for **resolving consumer disputes**

Another key feature of the Consumer Act is the establishment of the **Consumer Protection Advisory Committee**. The Committee's main functions include:

1. Advising the Cabinet Secretary
2. Formulating consumer protection policy
3. Promoting and/or participating in consumer protection programmes
4. Advising consumers on their rights and obligations under appropriate laws
5. Monitoring and reviewing business and trading practices

(ii)

Commentary

Cloud Policy

https://ict.go.ke/sites/default/files/2024-12/Kenya%20Cloud%20Policy%20-%202024_0.pdf

Kenya's **Cloud Policy** was issued by the Ministry of Information, Communications and the Digital Economy in 2024. The Policy is underpinned by the following objectives:

- to ensure a smooth transition from traditional on-premises data centre practices to Cloud Computing Technology; and;
- to facilitate cross-border transmissions and strengthen international collaboration, complementing other relevant existing cloud computing regulations.

Data / Privacy

https://new.kenyalaw.org/akn/ke/act/2019/24/eng@2022-12-31 (i)
https://www.odpc.go.ke/who-we-are/ (ii)

The **Data Protection Act 2019** covers the following areas:

- Establishing the Office of the Data Protection Commissioner
- Making provisions for the processing of personal data
- Stipulating the rights of data subjects and obligations of data controllers and processor

(i)

The Office of the Data Protection Commissioner **(ODPC)** is a government agency dedicated to ensuring the appropriate handling of personal data in Kenya, pursuant to the **Data Protection Act of 2019.**

Figure 26 Functions carried Kenya's ODPC

(ii)

Commentary

Fraud

https://new.kenyalaw.org/akn/ke/act/1977/1/eng@2023-12-11

The **Prevention of Fraud (Investments) Act 1997** (most recently amended in 2023) outlines provisions for persons dealing in securities and additionally, measures to prevent fraud in investments.

The main features of the Act are as follows:

1. Establishing a **New Issues Committee**, responsible for overseeing security issuance and ensuring compliance with national laws. This may involve refusing grant approvals or imposing certain conditions on securities issues.
2. **Regulating businesses dealing in securities**. This includes licencing requirements and the powers of the finance minister to create rules for regulating business conduct.
3. Fraud **prevention** measures.
4. The **authorization process** for stock exchanges and conditions for **dealer exemptions.**

Requirements of the public trustee (appointed under the Public Trustee Act) to establish, maintain and administer a compensation fund.

Sanctions

https://www.frc.go.ke/?page_id=193

As a UN Member State, Kenya is bound by the decisions and resolutions of the UN Securities Council. Therefore, Kenya is committed to implementing UNSCRs, including those pertaining to UN sanctions regimes.

Kenya also has its own **Domestic Targeted Financial Sanctions (TFS) regime**, which is administered by the Counter Financing of Terrorism Inter-Ministerial Committee.

TFS lists can be accessed via the **FRC website**.

At the time of writing only the UNSCR list was available for download.

Commentary

Terrorism

http://kenyalaw.org:8181/exist/rest//db/kenyalex/Kenya/Legislation/English/Acts%20and%20Regulations/P/Prevention%20of%20Terrorism%20Act%20-%20No.%2030%20of%202012/docs/PreventionofTerrorismAct30of2012.pdf (i)

https://counterterrorism.go.ke/ (ii)

https://new.kenyalaw.org/akn/ke/act/ln/2022/31/eng@2022-12-31 (ii)

The **Prevention of Terrorism Act** 2012 (most recently revised in 2023) makes provisions for the **detection and prevention** of terrorist activities, amending both Extradition Acts (Commonwealth and Contiguous and Foreign Countries).

The Act covers the following areas:

1. Specified entities i.e. entities that are suspected to be involved in terrorist activities will be listed as specified entities by the Cabinet Secretary for matters pertaining to internal security
2. Defining what constitutes as an act of terrorism and its corresponding penalties
3. Powers of the Police and other relevant authorities to investigate and convict terrorist offences
4. Counter terrorism measures which includes the establishment of the National Counter Terrorism Centre (**NCTC**) (i)

The NCTC is a multi-agency institution, responsible for *detecting, deterring and disrupting* terrorist acts. Some of their main functions include:

1. Blocking pathways to radicalisation and recruitment into violent extremism by implementing action plans, training programmes and other operations.
2. Coordinating multi-agency policies directed at detecting, deterring and disrupting terrorist operations and attacks.
3. Reviewing targets that may be vulnerable to terrorist attacks and upgrading their security.(ii)

Kenya has ratified the UN Conventions aimed at addressing terrorism and terrorism financing. Considering this, the Government issued the **Prevention of Terrorism (Implementation of the United Nations Security Council Resolutions on Suppression of Terrorism) Regulations.**

To implement the UN's Resolutions, the Regulation document establishes a **Counter Financing of Terrorism Inter-Ministerial Committee**. Their main functions are as follows:

1. Implement relevant UNSC Resolutions.
2. Formulate and supervise the implementation of the **National Strategy and Action Plan.** (iii)

Company Registrar

https://brs.go.ke/companies-registry/

The Business Registration Service **(BRS)** is Kenya's official company registrar.

Access to Public

https://www.kenyalaw.org/kl/index.php?id=9766

Kenya's **Access to Information Act 2016**, Part II, Section 4 provides that every citizen has the right to access information held by a state body, or another person where that information is required for the purposes of data protection.

Other

https://www.president.go.ke/ (i)

https://mfa.go.ke/ (ii)

Official website for the President of the Republic of Kenya. (i)

Ministry of Foreign & Diaspora Affairs. (ii)

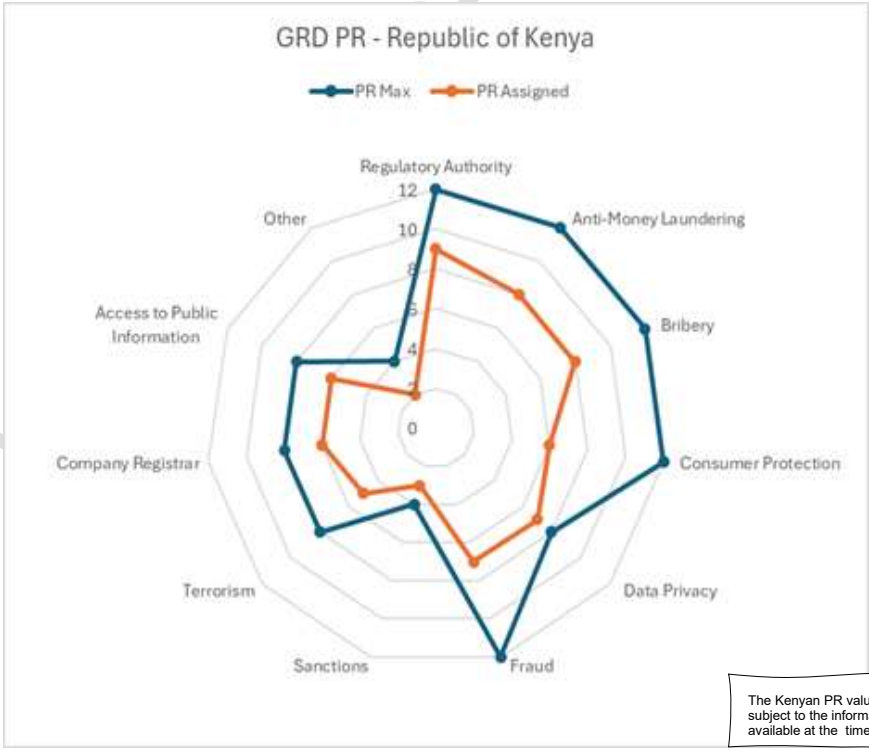
Posture Rating Kenya

The PR value of **6.7** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	9	8	8	6	7	7	3	5	6	6	2

Kenya has well-defined processes, regulations and laws which provide a measure of control when meeting any domain obligations.

NB: **The figure does not reflect the execution of any laws and regulations**.



Republic of Latvia

Commentary

Financial Regulatory Authority

https://www.bank.lv/en/ (i)
https://www.bank.lv/en/operational-areas/supervision/financial-market-supervision (ii)
https://www.bank.lv/en/about-us/integration-of-latvijas-banka-and-the-fcmc (iii)

Latvijas Banka is the central bank of Latvia.

The activities of Latvijas Banka are managed and overseen by the collegial authorities' committees and commissions. (i)

In accordance with the **Law on Latvijas Banka (2023)**, Latvia's Financial and Capital Market Commission (**FCMC**) was integrated with Latvijas Banka for the purpose of *creating one powerful and efficient institution* to govern the financial sector and economy of Latvia.

(ii)

Latvijas Banka regulates and supervises the operations of Latvia's financial markets by performing various functions. These include:

1. Issuing regulatory enactments and shaping policy guidelines for financial market participants
2. Stipulating the qualification and eligibility criteria for financial market participants and their officials
3. Collecting, analysing and publishing information pertaining to the financial market (iii)

The official currency of Latvia is the **euro.**

AI Act / Policy

https://artificialintelligenceact.eu/the-act/ (i)
https://ai-watch.ec.europa.eu/countries/latvia-0/latvia-ai-strategy-report_en (ii)
http://tap.mk.gov.lv/doc/2020_02/IZ_MI%5b1%5d.2.docx (iii)

As an EU Member State, Latvia is bound by the EU AI Act 2024.

(i)

Latvia's national AI strategy on Developing Artificial Intelligence Solutions was first issued in 2020, outlining Latvia's plan for promoting and increasing the uptake of AI across the whole economy.

The Strategy focuses on several key areas, including:

1. **Human Capital** i.e. up skilling the citizens of Latvia in AI-related fields to help accelerate the speed of AI deployment, use and development
2. **Research Projects in AI**, targeting priority sectors, such as transport, with high capacity for AI application
3. **Promoting collaboration with international organizations**, sharing achievements and best practices to increase opportunities for public-private partnerships in AI
4. Calls to develop a **normative regulatory framework** to help determine what is ethically and legally sound in the field of AI (ii)

The full version of the Latvian government's National AI Strategy can be downloaded from the European Commission's website.

(iii)

https://www.bank.lv/en/operational-areas/supervision/aml-cft/prevention-of-money-laundering-and-financing-of-terrorism-and-proliferation (i)

https://likumi.lv/ta/en/en/id/178987-law-on-the-prevention-of-money-laundering-and-terrorism-and-proliferation-financing (ii)

https://www.fm.gov.lv/en/progress-latvia-combatting-money-laundering-and-financing-terrorism?utm_source=https%3A%2F%2Fwww.bing.com%2F (iii)

The **Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing 2008** (most recently amended in 2024) is the most consequential piece of AML/CFT legislation in Latvia.

One of the main areas of focus in the AML/CFT law is **customer due diligence.** The Law requires customers of financial institutions (including banks) to provide any necessary information/documentation required for them to carry out risk-assessments (N.B. 'high-risk' customers will be required to provide more information and vice versa). If a customer fails to provide sufficient information/documentation, it is the duty of the financial institution to decide whether the business relationship needs to be terminated.

(i)

The full version of the legislation is available on the 'Legislation of the Republic of Latvia's' website.

(ii)

Considering recommendations made by an **FATF Mutual Evaluation report**, the Government of Latvia has implemented various measures to help strengthen their AML/CFT framework. These include:

1. **Effectively de-risking the financial sector**; amending the Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing, preventing banks and other payment institutions from cooperating with shell entities
2. **Improving investigation and prosecution processes**, including the establishment of a Financial Crime Investigation Task Force to facilitate more cooperation between the public and private sector regarding financial intelligence and investigations
3. **Strengthening the targeted financial sanctions (TFS) framework** e.g. broadening the scope of persons subject to TFS obligations

(iii)

Commentary

Bribery

https://www.knab.gov.lv/en/media/1701/download (i)

https://www2.mfa.gov.lv/en/eu/anti-corruption-measures-in-latvia (ii)

As stipulated in a progress report by the Corruption Prevention and Combatting Bureau, Latvia's **Criminal Law** sanctions bribery in its various forms:

1. Active and passive bribery (both in the public and private sector)
2. Misappropriation of a bribe
3. Giving or receiving bribes
4. Giving or receiving bribes on behalf of someone else

(i)

Latvia's **Corruption Prevention and Combatting Bureau** is the primary authority responsible for tackling corruption in Latvia.

The Bureau has three main focal points:

To achieve these goals, the Bureau seeks to do the following:

1. Continue aligning Latvia's national legislation with international anti-corruption instruments, e.g. the **OECD's Baltic Integrity Programme** (also known as the Baltic Anti-Corruption Initiative) and the **OECD CIME Working Group on Bribery in International Business**
2. Promoting partnerships between public and private institutions regarding corruption prevention

(ii)

Consumer Protection

https://www.ptac.gov.lv/en/consumer-protection (i)
https://www.em.gov.lv/sites/em/files/consumer_rights_protection_law1.doc (ii)

The **Consumer Rights Protection Centre (CRPC)** is responsible for enforcing the Consumer Rights Protection Law, Advertising Law, Law on the Safety of Goods and Services, Law on Information Society Services, as well as various other laws and regulations pertaining to consumer rights in Latvia.

The CRPC performs a range of functions, including:

1. Supervising and controlling the market e.g. supervising information about commodities and services, ensuring compliance with relevant laws and regulations
2. **Reviewing customer complaints** regarding consumer rights violations
3. **Protecting the economic interests of consumers** through the supervision of advertising, contracts' projects etc
4. **Representing consumer rights** in other fields e.g. the use of public services

(i)

The main law governing the CRPC is the **Consumer Rights Protection Law**. Some of the main features of the Law include:

1. Defining what constitutes as a consumer rights violation
2. Protecting consumer's freedom of choice
3. Prohibiting unfair contractual terms e.g. terms that contradict the principle of legal equality of contracting parties, this law, or other relevant regulations.
4. Consumer's right to withdraw from contracts
5. Access to information requirements regarding goods and services
6. Consumer rights protection associations
7. Functions and powers of the CRPC

(ii)

Cloud Policy

https://commission.europa.eu/projects/national-federal-cloud-latvia_en (i)
https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/02/going-digital-in-latvia_0cf1d1d6/8eec1828-en.pdf (ii)

The **National Federal Cloud of Latvia**, co-funded by the EU, aims to consolidate public sector data storage and computing capabilities in Latvia. The Federal Cloud integrates four key shared service providers:

1. Latvia Radio and Television centre.
2. The National Library of Latvia
3. The Ministry of Interior Affairs Information Centre
4. The Ministry of Agriculture into the national federated cloud

(i)

The OECD Review – **Going Digital in Latvia** outlines some key polices that Latvia has implemented as part of its digital transformation strategy. One of these is a project by **LITKA** (the Latvian Information and Communications Technology Association) entitled **Training of Small and Micro Entrepreneurs for Development of Innovations and Digital Technologies in Latvia**. The project, co-funded by the EU and the private sector, aims to fill some of Latvia's digital skills gaps, offering training in areas such as cloud services and security.

(ii)

Data / Privacy

https://www.dvi.gov.lv/en/about-us

The **Data State Inspectorate** is the supervisory authority responsible for implementing Europe's General Data Protection Regulation (**GDPR**) in Latvia.

The inspectorate operates independently, performing various functions, including:

1. Supervising the processing of personal data in line with relevant regulatory enactments
2. Proficiency checks of data protection officers and maintaining a register of qualified officers
3. Consulting public administration institutions regarding conformity of data processing systems with relevant regulatory enactments

Forwarding data subject's requests to the European Union Agency for Criminal Justice Cooperation (Eurojust).

Fraud

https://www.bank.lv/en/news-and-events/news-and-articles/news/17032-building-resilience-to-fraud-and-enhancing-digital-financial-literacy-with-eu-support-in-latvia-and-lithuania?template=centenary (i)

https://www.at.gov.lv/en/tiesu-prakse/judikaturas-nolemumu-arhivs/kriminallietu-departaments/klasifikators-pec-lietu-kategorijam/kriminalprocesa-likums (ii)

In 2024, **Latvija's Banka** came together with Lietuvos bankas, the European Commission, the OECD and other financial and security sectors to implement a new project with the aim increasing Latvia and Lithuania's financial security, sustainability and overall well-being. The project seeks to achieve this by strengthening the **financial digital literacy** of both country's populations, thus increasing their ability to **combat financial fraud.**

This project aims to enhance public financial security by:

1. **Raising awareness:** Educating individuals about the risks of fraud.
2. **Empowering individuals:** Providing information on digital financial tools that can help them identify and prevent fraud. (i)

As stipulated in the **Criminal Procedure Law of 2005,** any individual/entity accused of corruptive offences, including **fraud related to the financial interests of the EU**, shall be extradited to the relevant EU Member State.

(ii)

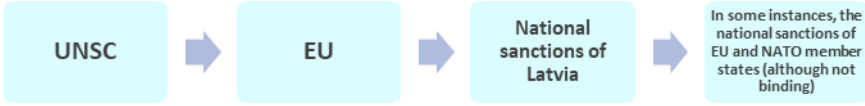
Sanctions

https://fid.gov.lv/en/roles-and-responsibilities/sanctions (i)
https://www.mfa.gov.lv/en/organization-security-and-cooperation-europe (ii)
https://sankcijas.fid.gov.lv/sankciju-mekletajs (iii)

As of April 2014, the **Financial Intelligence Unit of Latvia** were granted authority over the implementation of international and national sanctions.

(i)

Latvia is bound by the following sanctions:



(ii)

Full list of Latvia's targeted financial sanctions (**TFS**).

(iii)

Commentary

Terrorism

https://vdd.gov.lv/en/about/about-us (i)

https://vdd.gov.lv/en/areas-of-activity/counterterrorism (ii)

The **Latvian State Security Service (VDD)** is one of Latvia's three Security and Intelligence Services. One of its main focuses is coordinating and conducting counter-terrorism measures by gathering information from relevant sources, carrying out analysis and informing senior officials of any threats identified to national security. (i)

Some of the **preventative measures** implemented by the VDD to help combat terrorism include:

1. Putting **controls on immigration** from countries where terrorism threat-levels are high
2. **Regular inspections** of objects of critical infrastructure and soft targets
3. Preparing **recommendations** for the Government to improve the physical security of objects

The VDD has also developed and implemented the **National Counter-terrorism plan**. This sets out the preventative measures for institutions to follow, in accordance with **four threat levels.**

The National Plan takes into consideration security threats across Europe, focussing on some of the following areas:

1. Increasing security at mass gatherings
2. Preventing risks related to technology development
3. Protecting critical infrastructure objects
4. Increasing efficiency of information exchanges and reaction capacities of institutions engaged in counter-terrorism measures (ii)

Company Registrar

https://www.ur.gov.lv/lv/registre / (i)
https://www.ur.gov.lv/en/ (ii)
https://info.ur.gov.lv/#/notices-to-creditors/journal (iii)

The Latvian Government pages and service to register new companies. (i)

The Latvian company registrar can be searched via the Government website. (ii)

The Latvian Notifications to creditors, participants, interested parties (iii)

Access to public Information

https://likumi.lv/doc.php?id=50601

The **Freedom of Information Law 1998** (most recently amended in 2022) seeks to ensure that citizens of Latvia have access to public information, outlining procedures for the provision of information, re-use of information and protection of the rights of applicant for information.

Other

https://www.mk.gov.lv/en (i)

https://www.mfa.gov.lv/en?utm_source=https%3A%2F%2Fwww.google.com%2F (ii)

The Cabinet of Ministers website. (i)

The Ministry of Foreign Affairs website. (ii)

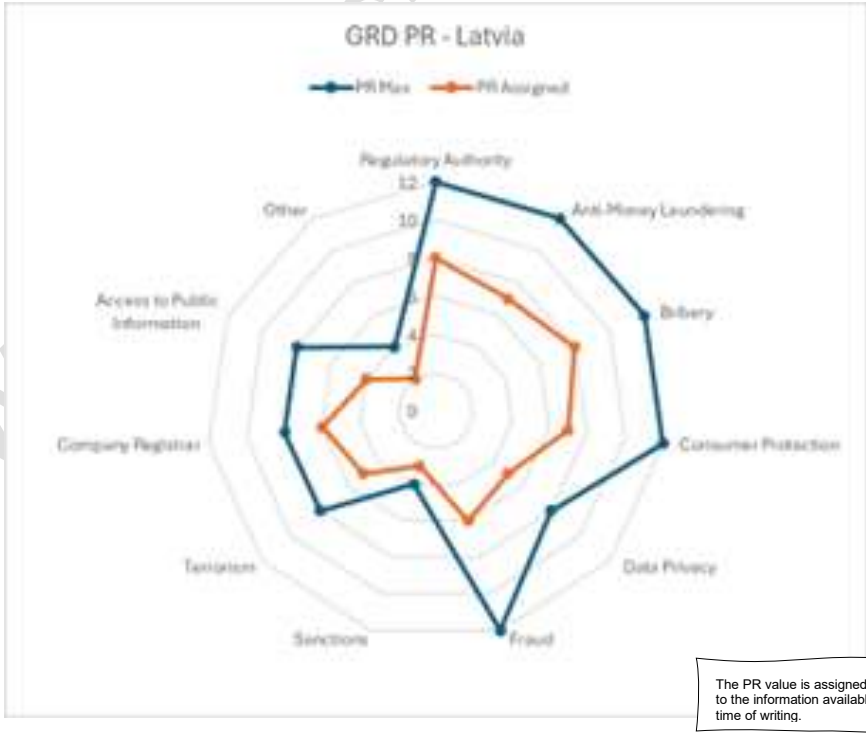
Posture Rating Latvia

The PR value of **6.1** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	8	7	8	7	5	6	3	5	6	4	2

Latvia has well defined processes, regulations and laws that provide a measure of control when meeting any domain obligations helped by the fact that it is a member of the EU.

NB: **The figure does not reflect the execution of any laws and regulations.**



The PR value is assigned subject to the information available at the time of writing.

Lebanon

Commentary

Financial Regulatory Authority

https://www.bdl.gov.lb/ (i)
https://bccl.gov.lb/

Banque du Liban (BDL) is the central bank of Lebanon. It was established on August 1, 1963 and became fully operational on April 1, 1964.

(i)

The BDL is a legal public entity, meaning it has full **financial and administrative autonomy**. As such, it is not subject to the same rules and controls applicable to other public sector institutions.

The main functions of the BDL include:

1. Issuing national currency
2. Regulating money supply
3. Controlling interest rates
4. Setting monetary policy
5. Supervising and developing the banking and financial sector

The Banking Control Commission of Lebanon (**BCCL**) was established in 1967 and is the supervisory authority of institutions licensed to operate in Lebanon: 57 banks, 36 financial institutions, 297 exchange institutions, credit counters and 20 electronic cash transfer companies at the time of writing.

(ii)

The currency in circulation in Lebanon is the Lebanese **pound .**

AI Act / Policy

https://omsar.gov.lb/Assets/DT_EN.pdf

Lebanon's **Digital Transformation Strategy** recognises AI as a key tool to be utilised in recovering the economy and restoring lost confidence. It seeks to do this via various means, including:

1. Engaging in consultations with major stakeholders regarding adopting emerging technologies, such as AI, to help drive efficiencies **in public service delivery**
2. Implementing the 2022 which introduces programming, robotics and AI to the school curriculum, helping to build human capital

Anti-Money Laundering

https://sic.gov.lb/sites/default/files/laws-regulations/Law%2044%20En.pdf (i)
https://sic.gov.lb/en/about-us (ii)

Law No 44 of November 24, 2015, **Fighting Money Laundering and Terrorist Financing** is the most consequential piece of legislation pertaining to combatting money laundering in Lebanon. Some of its main features include increasing the reporting obligations of financial institutions and the establishment of the **Special Investigation Commission (SIC).**

(i)

The **SIC** is Lebanon's Financial Intelligence Unit. They play an instrumental role in implementing Lebanon's **AML/CFT regime**, forming alliances with international partners and working to protect concerned sectors from illicit proceeds.

(ii)

Commentary

Bribery

https://omsar.gov.lb/Anti-corruption-(1)/Strategy-Execution-Plan (i)
https://nacc.gov.lb/wp-content/uploads/2023/11/P1E-Anti-Corruption-Commission-Law-175.2020.pdf **unofficial English translation** (ii)

In 2020, the **National Anti-Corruption Strategy Project** was implemented by the Lebanese Government. The Project combines the expertise of three authorities**:** legislative, executive and judicial, along with other relevant bodies from the public and private sector (e.g. municipalities and civil society bodies). Its overarching mission is to protect public funds from unnecessary loss/misuse (particularly in relation to implementing development programmes/projects) and ensuring all citizens of Lebanon have access to high-quality, trustworthy public services.

(i)

The main Law in relation to combatting bribery and corruption in Lebanon is the Law on Fighting Corruption in the Public Sector and the Establishment of the National Anti-Corruption Commission, 2020.

The Law seeks to **strengthen accountability and transparency** within the Lebanese Government, covering some of the following areas:

1. Defining the various forms of corruption
2. Strengthening reporting and accountability mechanisms
3. Establishing a **National Anti-Corruption Commission (NACC),** an independent regulatory authority responsible for investigating corruption offences, issuing recommendations for reform etc.

(ii)

Consumer Protection

https://www.economy.gov.lb/en/what-we-provide/consumer-protection/ (i)
http://www.economy.gov.lb/public/uploads/files/8282_2393_9984.pdf (ii)

The **Consumer Protection Directorate**, which falls under the jurisdiction of the Ministry of Economy and Trade, is the government body responsible for developing the **consumer protection framework** in Lebanon. Some of their main functions include:

1. Carrying out inspections of trade premises considering risk assessments
2. Consulting businesses on best practices regarding consumer protection
3. Investigating consumer complaints and offering advice where possible

(i)

The **Consumer Protection Law 2014** is the primary piece of legislation in Lebanon concerning consumer protection. One of its main features is the establishment of the **National Consumer Protection Council,** comprised of general managers of a few relevant ministries and representatives of the chambers of commerce, industry, agriculture, industrialists and advertising companies. The main purpose of the council is to ensure state departments take a **coordinated approach** in their implementation of the Consumer Protection Law.

(ii)

Commentary

Cloud Policy

https://omsar.gov.lb/Assets/DT_EN.pdf

As outlined in Lebanon's **Digital Transformation Strategy**, the Government has adopted a **Cloud-First Policy** i.e. choosing to adopt cloud solutions as default and only opting for other solutions where this isn't possible.

The Lebanese Government also recognises the additional risks that come with adopting a cloud computing solution. Hence, a key focus within their cloud strategy is to work with government agencies, key stakeholders and private cloud computing providers to devise a comprehensive framework to ensure they have the capacity to assess risk levels and implement appropriate controls.

Data / Privacy

https://omsar.gov.lb/Assets/docs/EtransactionLaw.pdf

Lebanon's **E-transaction Law and Protection of Personal Data** makes provisions for the collection, processing, or use of personal data. This applies to both electronic data as well as data in its various other forms.

The Law **does not** establish an independent judicial body to monitor the implementation and compliance of data protection regulations.

Fraud

https://sic.gov.lb/sites/default/files/laws-regulations/Law%2044%20En.pdf

Lebanon legislates against fraud in the Law on Fighting Money Laundering and Terrorist Financing. The Law stipulates that fraud, including fraudulent bankruptcy and fraudulent trading in counterfeit goods, are classified as illicit funds and hence may be investigated by the Special Investigation Commission.

Sanctions

As a UN Member State, Lebanon is bound by the UN Security Council Consolidated sanctions list.

Terrorism

https://isf.gov.lb/ar/strategic-plan/

The **Internal Security Forces (ISF)** is comprised of several units, including the General Inspectorate, Embassy Security Service and Beirut Police.

One of the key strategic objectives of the ISF, as outlined in the **ISF Strategic Plan 2018-2022**, is to enhance security, safety and stability by confronting terrorism and combatting crime.

Company Registrar

http://investinlebanon.gov.lb/en/doing_business/starting_a_business (i)

http://cr.justice.gov.lb/desc/desc.aspx (ii)

Guidance for foreign investors and Lebanese nationals on how to establish a business in Lebanon.

(i)

Where to search the company registrar of Lebanon.

(ii)

Commentary

Access to Public Information

https://nacc.gov.lb/wp-content/uploads/2023/11/P1E-Access-to-Information-Law-28.2017.pdf (**unofficial English translation**)

The **Access to Information Law** was first enacted in 2017, granting any natural or legal person, regardless of their standing or interest, the right to access public information. The Law also introduces the requirement for all state departments to appoint an **Information Officer**, responsible for collecting and in some instances publishing, requested information.

Although the 2017 Law brought in significant reforms to Lebanon's access to information legislation, there are still several challenges that may be presented to those requesting information e.g. strict limitations on the re-use of information.

Other

http://www.presidency.gov.lb/English/Pages/default.aspx (i)

https://www.ministryinfo.gov.lb/en/ (ii)

The official website of the President of Lebanon.

(i)

The Ministry of Information website.

(ii)

Posture Rating Lebanon

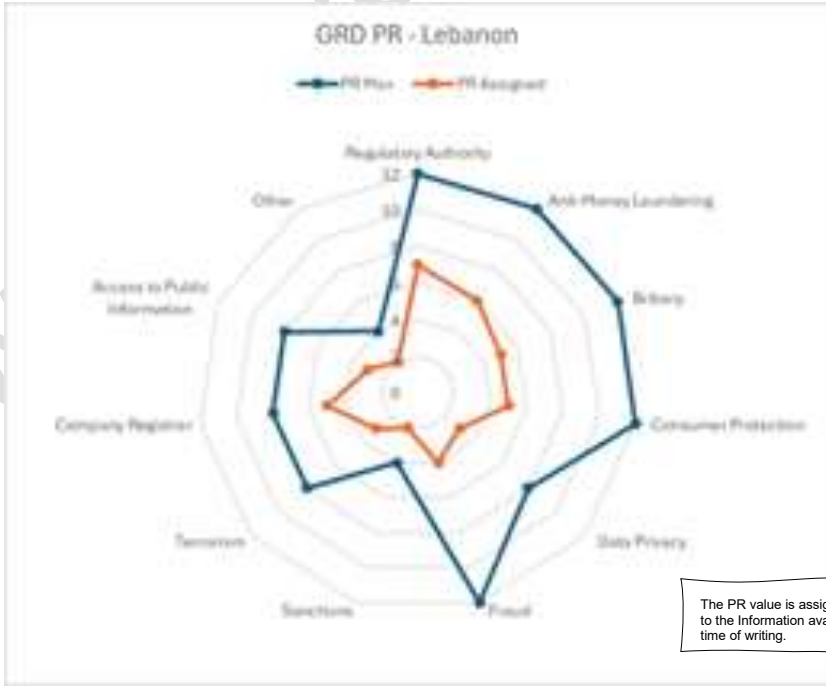
The PR value of **4.5** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	7	6	5	5	3	4	2	3	5	3	2

Lebanon has numerous processes, regulations and laws which provide a measure of control when meeting any domain and international obligations. The lack of unified digital channels to support the domains is reflected in the assigned value.

We observed minor integrity issues for URLs when validating the links through our checker and subsequently updated/removed some core links where appropriate.

NB: **The figure does not reflect the execution of any laws and regulations**.



Lithuania (Republic of)

Commentary

Financial Regulatory Authority

https://www.lb.lt/en/functions (i)
https://www.lb.lt/en/supervision-of-financial-market-participants (ii)
https://www.lb.lt/en/inspection-plans (iii)

The Bank of Lithuania (**Lietuvos bankas**) is the Lithuanian central bank. The Bank is comprised of nine departments, all responsible for carrying out the central bank's core functions. These are as follows:

1. Banking and Insurance Supervision
2. Financial Market Supervision
3. Legal and Licensing
4. Market Operations
5. Market Infrastructure
6. Financial Stability
7. Economics Department
8. Data and Statistics Department
9. Cash Department

Various divisions work under the umbrella of the above departments. (i)

Supervision of financial market participants is a primary focus of Lietuvos bankas. They currently supervise over **800 financial market participants**, including banks, credit unions, insurance undertakings, payment institutions etc. The Bank operates under a risk-based approach i.e. allocating resources towards the most significant financial market participants / those with the highest risk levels. (ii)

The Bank conducts two types of inspections of financial market participants: routine inspections, for which a plan is published to ensure transparency and promote efficiency and unannounced inspections, often carried out in collaboration with ECB experts if the participant is under their direct supervision. (iii)

Lietuvos bankas is the Lithuanian member of the Eurosystem becoming a member in 2015, at which point the **euro** replaced the national currency (litas).

AI Act / Policy

https://eimin.lrv.lt/uploads/eimin/documents/files/DI_strategija_ENG(1).pdf

The Lithuanian Artificial Intelligence Strategy, 2019 aims to "*modernise and expand the current AI ecosystem*" in Lithuania with the following objectives that underpin the strategy:

1. Build the National and international AI network
2. Ethical and legal principles
3. Integration
4. Skills Development
5. AI R&D
6. Standards

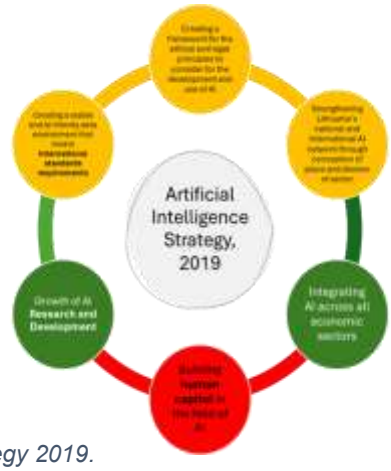


Figure 27 - Lithuania AI Strategy 2019.

Commentary

Anti-Money Laundering

https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/2c647332ba5111eb91e294a1358e77e9?jfwid=twcznlk4w (i)

https://fntt.lrv.lt/en/money-laudering-prevention/activites/ (ii)

The Republic of Lithuania **Law on the Prevention of Money Laundering and Terrorist Financing** serves the following purposes:

1. **Establishing** measures for combatting money laundering and terrorist financing in Lithuania
2. **Designating** institutions responsible for imposing of AML/CFT measures
3. **Implementing** relevant EU AML/CFT legal acts

(i)

The **Financial Crime Investigation Service** is Lithuania's Financial Intelligence Unit and is the main authority responsible for implementing the country's AML/CFT measures. Some of their **main activities** include:

1. **Collecting** and recording information regarding monetary operations and transactions of customers
2. **Analysing** and publishing information related to AML/CFT prevention measures
3. **Consulting** law enforcement and other state institutions about monetary operations and transactions carried out by customers
4. **Evaluating** legal acts and submitting proposals in line with international standards and recommendations

(ii)

Bribery

https://www.stt.lt/data/public/uploads/2021/09/law-on-corruption-prevention-new_2021.pdf (i)
https://tm.lrv.lt/en/corruption-prevention/ (ii)

The **Law Amending the Republic of Lithuania Law on Corruption Prevention 2021** was issued primarily to strengthen the existing Prevention of Corruption Law. It seeks to achieve this by outlining measures for improving national security, creating an anti-corruption environment and stipulating the powers and duties of corruption prevention bodies.

The Law regulates bribery in its various forms, including:

1. Trading in influence (***accepting*** a bribe)
2. Abuse of office (***giving*** a bribe)
3. Seeking acceptance or giving of a bribe
4. Concealing or disguising acceptance or giving of a bribe
5. Bribery of an intermediary (i)

As stipulated in the Law on the Prevention of Corruption, the **Special Investigation Service (STT)** is the statutory law enforcement institution accountable for detecting and investigating corruption and bribery offences in Lithuania.

After several Law amendments and analyses of anti-corruption activities, the STT's functions now also extend to the following areas:

1. Developing and implementing corruption prevention measures
2. Raising awareness and educating the public on corruption detection
3. Examining public requests and complaints (ii)

Commentary

Consumer Protection

https://e-seimas.lrs.lt/portal/legalActPrint/lt?jfwid=i3h7wscwc&documentId=e86e8310231911e6acbed8d454428fb7&category=TAD (i)

https://vvtat.lrv.lt/en/about-authority/ (ii)

https://ecc.lt/en/european-consumer-centre-lithuania/ (iii)

The most significant consumer protection law in the Republic of Lithuania is **the Law on Consumer Protection 1994** (most recently amended 2016).

The main features of the Law are as follows:

1. Defining consumer rights and the scope of protection
2. Establishing an institutional system for the protection of consumer rights
3. Powers and duties of competent consumer rights protection authorities
4. Supervising the education of consumers, relations between consumers and sellers, suppliers of services, protection of consumers out of court and liability for violations of legal acts related to consumer protection

(i)

The **State Consumer Rights Protection Authority (SCRPA)** sits within the Ministry of Justice and is the government agency responsible for enforcing consumer policy in Lithuania. Their main functions include:

1. **Enforcing consumer policy** in areas such as unfair commercial practices, misleading advertising, e-commerce etc.
2. Serving as the main alternative dispute resolution body (**AGS**)
3. **Monitoring activities** in other fields to help prevent consumer protection infringements
4. **Organising educational** activities for consumers, traders and service providers
5. Acting as the main competent service for the implementation of **EU regulations**, including Regulation **(EC) No 2017/2394** on consumer protection cooperation and Regulation **(EU) No 524/2013** on online dispute resolution for consumer disputes

(ii)

As an EU Member State, Lithuania has also established the **European Consumer Centre Lithuania**, which has been operating since 2005. The Centre works in collaboration with the European Consumer Centre Network (**ECC-Net**) to advise citizens on their rights as consumers and provide easy access to redress, particularly in cross-border cases.

(iii)

Cloud Policy

https://eimin.lrv.lt/uploads/eimin/documents/files/Lithuanian%20Industry%20Digitisation%20Roadmap%202020-2030%20UPDATED%20EN%20(1).pdf

---

One of the key features within the Lithuanian Industry **Digitisation Roadmap 2020-2030** is the **Industrial Internet of Things (IIoT)** project. The premise of this project is to utilise cyber-physical systems (CPS), big data and cloud computing to create new business models, increase productivity and exploit data analytics to **transform the workforce** in Lithuania.

Another key project is **Cloud Manufacturing (CMfg),** a model which aims to enhance efficiency, reduce product lifecycle costs and optimise resource allocation.

Commentary

Data / Privacy

https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/ef70b5d2f14811e78f3dc265493430ae (i)

https://vdai.lrv.lt/en/services/ (ii)

The Republic of Lithuania Law on **Legal Protection of Personal Data 1996** *(most recently amended in 2016*) fully implements the EU's **GDPR** into its legal system. The primary purpose of the Law is to safeguard individual rights concerning the processing of personal data.

Some of the main features of the Law are as follows:

1. Processing of personal data
2. Rights of the data subject
3. Security of data
4. Registration process for data controllers
5. Transferring data to recipients in foreign countries
6. Functions of relevant authorities in shaping data protection policy and implementing the Law, i.e. the roles of the Ministry of Justice and the State Data Protection Inspectorate

(i)

The **State Data Protection Inspectorate** is the main authority responsible for monitoring the application of **GDPR** and the **Law on Legal Protection of Personal Data**. Furthermore, they are the primary contact for individuals seeking information regarding their rights regarding the use and processing of their personal data. N.B. **Information request forms** are available via the Inspectorate's official website.

(ii)

Fraud

https://latlit.eu/about-the-programme/anti-fraud-policy/

Latvia-Lithuania's Anti-Fraud Programme 2021-2027, otherwise known as the Managing Authority (**MA**), Joint Secretariat (**JS**), Latvian National Authority and Lithuanian National Authority of the Interreg VI-A Latvia – Lithuania Programme (**MA/JS Programme)**, seeks to promote a culture which deters fraud and facilitates the prevention and detection of fraud.

The Programme is **co-funded by the EU** and hence, the MA/JS works closely with the EU Anti-Fraud Office and the European Prosecutor's Office to investigate and report suspected fraud cases.

The Financial Crime Investigation Service operates under the Ministry of the Interior of the Republic of Lithuania and is one of the leading authority's responsible for investigating financial crimes such as fraud.

Sanctions

https://www.urm.lt/en/sanctions

Lithuania is bound by the sanctions imposed by the **EU and UN.**

The **Ministry of Foreign Affairs** is responsible for the implementation of international sanctions.

Commentary

Terrorism

https://rm.coe.int/profile-lithuania-may-2021-1-2768-1133-2099-v-1/1680a2b115 (i)
https://www.urm.lt/en/lithuania-in-the-region-and-the-world/lithuanias-security-policy/nuclear-and-cyber-security-fight-against-terrorism/999 (ii)

Council of Europe's Report on **Lithuania's Counter-Terrorism Capacity** outlines some of the key measures implemented by Lithuania to combat terrorism. For example, it highlights the **Public Security Development Programme 2015-2025** which has a key objective of reducing (and eradicating where possible) the potential risk factors associated with terrorism. To achieve this objective, the Programme established an **inter-institutional working group** to address issues concerning the fight against terrorism and its financing.

As stated in the Report, there is currently **no standalone anti-terrorism law** in Lithuania. Instead, criminal liability for terrorist offences is covered in **Lithuania's Criminal Code.** That said, Lithuania has adopted the Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania (**LPMLTF**), which seeks to prevent money laundering and/or terrorist financing as well outlining the duties and powers of relevant authorities.

(i)

Some of Lithuania's key contributions regarding countering terrorism on an **international level** include:

1. Actively participating in the **international counter-terrorism frameworks**, e.g. chairing the EU Council working parties on internal and external counter-terrorism aspects, and
2. Commencing a **two-year term on the UNSC** from Jan 2014, taking over the Presidency of the Council's **Counter-Terrorism Committee** and its relevant Working Group

(ii)

Company Registrar

https://www.registrucentras.lt/en/ (i)
https://www.registrucentras.lt/jar/p/pav.php (ii)

The Lithuanian state enterprise centre of registers. (i)
Link to search the Lithuanian company registrar via the **Registru Centras** website. (ii)

Access to Public Information

https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/b4e14de06a3811ecb2fe9975f8a9e52e?jfwid=-2y4hh7oyd

The Law on the Provision of Information to the Public 1996 (most recently amended 2021) outlines the procedures for collecting, producing, publishing and disseminating public information as well as the rights, duties and liability of producers and disseminators of public information.

According to **Chapter II of the 1996 Law**, all citizens of Lithuania have the right to '*collect, obtain and disseminate information*', subject to a few exceptions i.e. if the information poses a threat to the '*constitutional system, a person's health, honour, dignity, private life and morality*.'

Other

https://lrv.lt/en/

The official portal of the Government of Lithuania.

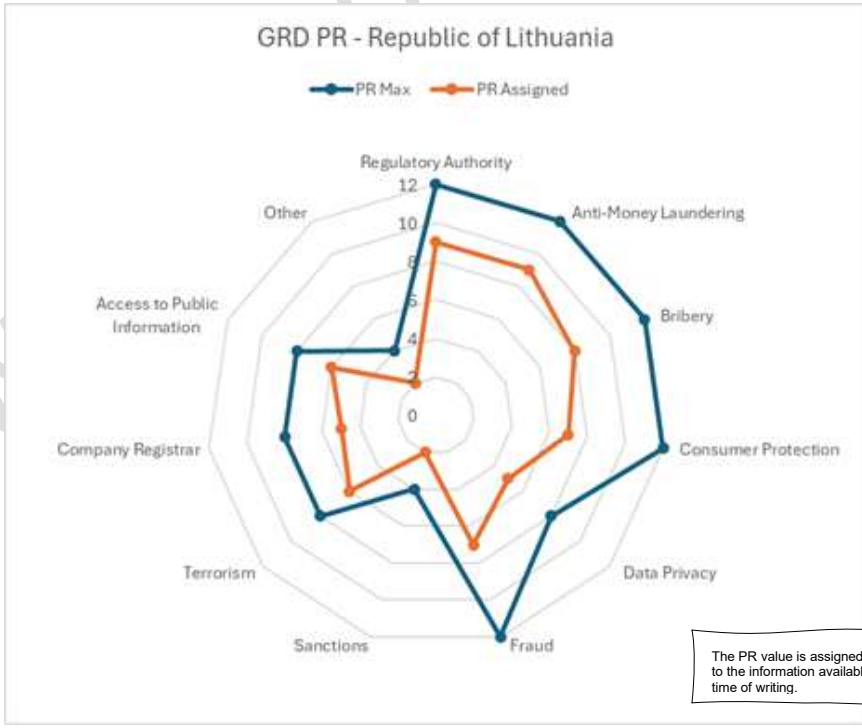
Posture Rating - Lithuania

The PR value of **6.6** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	9	9	8	7	5	7	2	6	5	6	2

Having adopted many EU practices, the Republic of Lithuania has defined processes, regulations and laws that provide a degree of control when meeting its obligations. The value reflects the available information at the time of writing.

NB: **The figure does not reflect the execution of any laws and regulations.**



Luxembourg

Commentary

Financial Regulatory Authority

https://www.bcl.lu/en/index.html (i)
https://www.cssf.lu/en/about-the-cssf/ (ii)
https://www.cssf.lu/en/whistleblower-protection/ (iii)

The Banque Centrale du Luxembourg (**BCL**) is the monetary authority of Luxembourg and a member of the Eurosystem and the European System of Central Banks (**ESCB**).

The BCL has institutional, operational and personal independence. The State is still the sole holder of the BCL's capital; however, its independence is guaranteed through relevant laws and treaties.

Pursuant to the **Organic Law of the BCL**, the Bank's primary focus is to carry out the **tasks of the ESCB** and help fulfil its objectives. As such, the BCL's main functions are as follows:

1. Defining and implementing monetary policy
2. Conducting foreign exchange transactions
3. Holding and managing the official foreign exchange
4. Promoting the proper functioning of payment systems

(i)

The Commission de Surveillance du Secteur Financier (**CSSF**) is a public body, responsible for supervising the professionals and products of the Luxembourg financial sector e.g. credit institutions, investment firms, payment institutions etc. Some of their main functions include:

1. Ensuring authorised entities are compliant with regulations applicable to them
2. Representing Luxembourg in European and international supervision
3. Public oversight of the audit profession
4. Financial consumer protection

(ii)

The CSSF has **whistle blower protection**, meaning any private or public sector entity (amongst others) can report a breach of national and/or EU law without risk of retaliation.

(iii)

AI Act / Policy

https://mindigital.gouvernement.lu/en/axes.html

Luxembourg's **Ministry of Digitisation** has committed to encouraging digitalisation and innovation in the public sector by promoting recent technologies such as Distributed Ledgers (blockchain), AI and the Internet of Things (IoT).

Commentary

Anti-Money Laundering

https://mj.gouvernement.lu/en/dossiers/2020/lutte-blanchiment.html (i)
https://mj.gouvernement.lu/dam-assets/dossiers/blanchiment/en-nra-import-version-2982022.pdf (ii)
https://www.cssf.lu/en/anti-money-laundering-and-countering-the-financing-of-terrorism/#cssf-approach-with-respect-to-aml-ctf (iii)

The Directorate for Combating Money Laundering and the Financing of Terrorism (**AML/CFT Directorate**) falls under the jurisdiction of the Ministry of Justice.

Some of the Directorate's main duties include:

1. **Representing Luxembourg at FATF meetings**, contributing to the development of international best standards and preparing for FATF mutual evaluations
2. Participating in various **European AML working groups**
3. Coordinating **AML/CFT efforts on a national level,** updating the national AML/CFT risk assessments and directing various committees
4. **Shaping AML/CFT legislation**, participating in the negotiation of regulations and directives forming the *"anti-money laundering and anti-terrorist financing package"* proposed by the Commission

(i)

The **National Risk Assessment of Money Laundering and Terrorist Financing** was issued by the Ministry of Justice in 2020 to identify specific threats and vulnerabilities to ML/TF in Luxembourg, helping to formulate effective AML/CFT measures.

Given its risk-based approach, particular focus is placed on risks stemming from Luxembourg's position as a global financial centre which is crucial because the financial sector dominates Luxembourg's economy, hosting numerous foreign institutions and assets and serves as a leading Eurozone hub for international financial services.

(ii)

The **CSSF** is Luxembourg's primary AML regulator, responsible for ensuring all entities under their supervision are compliant with their AML/CFT obligations.

The CSSF works closely with Luxembourg's Financial Intelligence Unit (**FIU**) when investigating AML/CFT cases, both exchanging information with one another where necessary.

(iii)

Bribery

https://legilux.public.lu/eli/etat/leg/code/penal/20240308#section_18 (i)
https://www.oecd.org/en/topics/sub-issues/fighting-foreign-bribery/luxembourg-country-monitoring.html (ii)

Luxembourg criminalises bribery and corruption in its various forms through the **Penal Code**. This includes:

- Article **246** – Passive bribery involving a public agent or force
- Article **247** – Active bribery involving a public agent or force
- Article **248** – Influence peddling, i.e. abusing one's power by giving or receiving a bribe to gain authorisation or influence a public entity (i)

Luxembourg is a Party to the **OECD Anti-Bribery Convention** and, hence, is subject to rigorous peer-review monitoring to assess the efficacy of its anti-bribery and corruption measures.

(ii)

Commentary

Consumer Protection

https://mpc.gouvernement.lu/en/le-ministere/protjur.html (i)
https://mpc.gouvernement.lu/en/dossiers/2023/codeconsommation.html (ii)

The Directorate for Consumer Protection negotiates European documents and draft laws, transposing them into national legislation and the **Code of Consumption.**

(i)

The primary objective of the **Code of Consumption** is to protect consumers and promote balanced relationships between different parties.

The Code offers **consumers and professionals** information concerning their **rights and duties** under consumer protection law, covering the following areas:

1. Mandatory information that must be provided to consumers by professionals on the goods and services that they sell
2. Price indication requirements
3. Unfair trading practices
4. Consumer contract rules and regulations
5. Roles of consumer protection and mediation authorities
6. Rules on penalties

The **Consumer Council of Luxembourg** is an advisory body, comprised of representatives from the Government, consumer protection bodies and employers. Their main goal is to encourage the exchange of views and consultations between its members on issues regarding consumer protection.

(ii)

Cloud Policy

https://innovative-initiatives.public.lu/stories/cloud-strategy-accompanying-governments-digital-transformation

In line with the Government's **digital transformation programme**, the Grand Duchy of Luxembourg announced the adoption of a new strategy in relation to its use of Cloud technologies.

The foundation of the strategy is for Cloud technologies to be utilised by public administrations in Luxembourg to help cut *costs* and drive *efficiencies*. To achieve this, the Government has launched a project called '**govCloud'**, which focuses on a private cloud architecture, managed by the State's Information Technology Centre**.**

Data / Privacy

https://cnpd.public.lu/en/commission-nationale/organisation.html (i)
https://cnpd.public.lu/en/legislation/droit-lux.html (ii)

The National Commission for Data Protection (**CNPD**) has a range of duties in accordance with the EU's **GDPR**. These include:

1. Monitoring and enforcing GDPR in Luxembourg
2. Informing controllers and processors of their obligations and duties under GDPR
3. Promoting public awareness of the risks, rules, safeguards and rights in relation to data processing

(i)

More information about Luxembourg's national data protection legislation is available on the **National Commission for Data Protection's** website.

(ii)

Commentary

Fraud

https://anti-fraud.ec.europa.eu/policy/policies-prevent-and-deter-fraud/european-public-prosecutors-office_en?prefLang=nl (i)

https://legilux.public.lu/eli/etat/leg/code/penal/20240308#section_18 (i)

Luxembourg is one of the participating countries in the **European Public Prosecutor's Office**, a European-wide body that tackles large-scale, cross-border crime against the EU budget. This includes offences such as fraud, corruption or serious cross-border VAT fraud.

(i)

There aren't any specific standalone laws against fraud in Luxembourg. Instead, the various types of fraud and subsequent penalties can be found in the **Penal Code.**

(ii)

Sanctions

https://mfin.gouvernement.lu/en/dossiers/2018/sanctions-financiaires-internationales.html (i)

https://legilux.public.lu/eli/etat/leg/loi/2020/12/19/a1072/jo (ii)

Luxembourg implements the following sanctions lists:

- EU Consolidated list of sanctions
- UN Sanctions

The above is available for viewing on the www.kyc-data.com portal.

The **Ministry of Finance** is the competent authority responsible for implementing financial restrictive measures in Luxembourg.

(i)

Luxembourg has a national framework for implementing EU and UN restrictive measures, as outlined in the **Law of December 19, 2020**. Some of the main legal acts, resolutions and regulations referred to include:

1. Prohibition or restriction of financial activities
2. Prohibition or restriction on the provision of financial services, technical assistance, training or advice concerning a state
3. Freezing of funds, assets or other economic resources

(ii)

Commentary

Terrorism

https://mj.gouvernement.lu/dam-assets/dossiers/blanchiment/tf-vra-2022-en.pdf (i)
https://www.cssf.lu/en/anti-money-laundering-and-countering-the-financing-of-terrorism/#cssf-approach-with-respect-to-aml-ctf (ii)
https://hcpn.gouvernement.lu/en/service/attributions.html (iii)

The Terrorist Financing Vertical Risk Assessment (**VRA**) was adopted by the Prevention of Money Laundering and Terrorist Financing (**the Prevention Committee**) in May 2022. The aim of this was to provide a deeper understanding of the key drivers behind terrorist financing, following the approach outlined in the FATF **TF Risk Assessment Guidance (2019).**

(i)

The **CSSF** is responsible for ensuring all persons/entities under their supervision, authorisation, or registration fulfil their counter-terrorist financing obligations.

The powers and duties of the CSSF include:

1. Being entitled to access any documents deemed necessary to exercise their supervisory and investigative powers
2. Imposing administrative sanctions in the case of non-compliance
3. Issuing broader sanctions such as warnings, reprimands, administrative fines or occupational prohibitions against persons subject to its AML/CTF supervision (ii)

The High Commission for National Protection (**HCPN**) is responsible for coordinating Luxembourg's counter-terrorism measures (amongst various other duties). The HCPN's legislative and regulatory texts can be found on their official website (***only available in French***). (iii)

Company Registrar

https://www.lbr.lu/mjrcs/jsp/IndexActionNotSecured.action?time=1708599365925&loop=2 (i)
https://www.lbr.lu/mjrcs/jsp/secured/DisplaySearchEBRActionV2.action?currentMenuLabel=menu.item.ebrsearchv2&FROM_MENU=true&time=1708599368796 (ii)

Legislation and forms to register a new business in Luxembourg, the Registre De Commerce Et Des Societies (**RCS**). (i)

The online service for searching the Luxembourg company registrar. (ii)

Access to Public Information

https://cnpd.public.lu/en/particuliers/vos-droits/droit-acces.html (i)
https://data.public.lu/en/ (ii)

Luxembourg's **Open Data Strategy** ensures that all public data (with a few exceptions, e.g. data relating to national security and data containing personal information) should be **open to the public by default**. This is in line with the EU's legislative framework of the **Open Data movement**. (i)

The **National Open Data portal** provides easy access to public sector data for individuals and businesses, covering areas such as geospatial data, environmental data and public health data. (ii)

Other

https://gouvernement.lu/en.html (i)
https://guichet.public.lu/en/citoyens.html (ii)

The official Government website. (i)

Guichet.lu is a government website which provides information, procedures and services offered by Luxembourg public bodies. (ii)

Posture Rating - Luxembourg

The PR value of **7.1** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	10	9	7	8	6	7	3	5	6	7	3

Situated in the heart of Europe and the EU, Luxembourg aligns with EU practices, subsequently defining its processes, regulations and laws. This provides a measure of control when meeting its obligations.

NB: **The figure does not reflect the execution of any laws , regulations or processes.**

Malaysia

Commentary

Financial Regulatory Authority

https://www.bnm.gov.my/

Bank Negara Malaysia (the Central Bank of Malaysia). Bank Negara Malaysia is governed by the **Central Bank of Malaysia Act 2009.**

The primary function of the Bank is to implement Malaysia's **monetary policy**. However, they also carry out various other activities, including:

1. Maintaining a stable financial system
2. Assisting in developing financial system infrastructure
3. Acting as a banker and adviser to the Government
4. Issuing currency and managing the country's international reserves
5. Implementing measures to raise the level of financial literacy amongst consumers

The currency of Malaysia is the Malaysian **ringgit**.

AI Act / Policy

https://www.malaysia.gov.my/portal/content/30613

One of the key initiatives of the Government's Big Data Programme is the implementation of machine learning to assist policymakers in determining the direction of the country. As such, the Malaysian Government has committed to providing civil servants with training on the application of **machine learning and AI in public services.**

Anti-Money Laundering

https://www.sc.com.my/amla/overview-of-the-amlcftcpf-regime (i)
https://amlcft.bnm.gov.my/bank-negara-malaysia-as-the-competent-authority (ii)
https://www.sprm.gov.my/admin/files/sprm/assets/pdf/penguatkuasaan/amlatfpuaa-2001-akta-613-bi.pdf (iii)

Malaysia's most consequential AML/CFT law is the Anti-Money Laundering and Terrorist Financing Act 2001 **(AMLA).** Some of its main features include:

1. Defining what constitutes a money laundering offence
2. Outlining ML/TF prevention measures e.g. customer due diligence and suspicious transaction reporting requirements
3. Forfeiture of property
4. Establishment of a competent Financial Intelligence Unit (FIU)
5. Reporting obligations of institutions
6. International cooperation (i)

As specified in the AMLA, **Bank Negra Malaysia** is the competent authority responsible for implementing Malaysia's AML/CFT regime. This includes covering areas such as:

1. **Financial Intelligence** (the FIU sits within Bank Negra Malaysia)
2. **Investigation and enforcement** of AML/CFT laws
3. **Supervision** of reporting institution (ii)

The Securities Commission Malaysia **(SC)** also plays a key role in enforcing AML/CFT measures in Malaysia, focusing solely on the financial sector.

The SC's AML/CFT regime is underpinned by **five key principles** as depicted below; (iii)

Figure 28 Malaysian AML/CFT regime key principles

Bribery

https://www.sprm.gov.my/admin/files/sprm/assets/pdf/penguatkuasaan/act-694-bi.pdf (i)
https://www.sprm.gov.my/index.php?page_id=75&articleid=463&language=en (ii)

The Malaysian **Anti-Corruption Commission Act 2009** outlines the penalties in place for the following bribery offences:

1. Bribery of a **public** body officer (**section 21**)
2. Bribery of **foreign** public officials (**section 22**)

It also outlines the duty of all persons to report bribery transactions and the penalties in place for those who intentionally fail to do so (**section 25**).

(i)

The Malaysian Anti-Corruption Commission **(MACC)** is an independent regulatory body, authorised by the Anti-Corruption Commission Act 2009 to investigate and prevent any form of corruption and abuse of power in Malaysia. Their main functions are as follows:

1. Receiving and handling reports/complaints concerning bribery or corruption
2. Conducting investigations
3. Offering consultancy/advisory services to drive system improvements
4. Enlisting support and educating the community on issues related to corruption (ii)

https://www.kpdn.gov.my/en/corporate-info/function-kpdn (i)
https://www.kpdn.gov.my/en/faq/tribunal-for-consumer-claims (ii)
https://lom.agc.gov.my/ilims/upload/portal/akta/outputaktap/1690994_BI/011121_Act%20599_final.pdf (ii)

The **Ministry of Domestic Trade & Cost of Living** is the government body responsible for enhancing consumer awareness and consumer protection in Malaysia. Additionally, they carry out consumer education programmes and encourage and assist consumer movements.

(i)

The **Tribunal for Consumer Claims** falls under the jurisdiction of the Ministry of Domestic Trade and Cost of Living. Their main objectives are as follows:

1. Offer consumers an accessible, convenient and low-cost alternative to civil courts for resolving disputes over purchased goods and services
2. Resolve claims independently and fairly
3. Help shape and develop laws on consumer protection

Information on '**how to file a claim'** is available on the Ministry's website.

(ii)

The Consumer Protection Act 1999 **(CPA)** is the main law governing consumer protection in Malaysia. The Act covers a range of areas, including:

1. Misleading and deceptive conduct
2. Safety of goods and services
3. Unfair contract terms
4. Guarantees concerning the supply of goods and services
5. Product Liability
6. Redress mechanisms e.g. establishing the Tribunal for Consumer Claims
7. Other provisions such as advertising, packaging and labelling, E-commerce etc.

(iii)

Commentary

Cloud Policy

https://www.pmo.gov.my/2024/10/pm-anwar-unveils-national-cloud-policy-focus-on-four-key-areas/ (i)

https://www.malaysia.gov.my/portal/content/31183 (ii)

In 2024, Malaysia's Prime Minister unveiled the **National Cloud Policy**. This focuses on four key areas:

1. Public service innovation and efficiency
2. Economic competitiveness and growth
3. Fuelling economic expansion
4. Strengthening user trust and data security

To achieve these objectives, the government plans on utilising cloud technology to modernise operations, promote citizen engagement and drive efficiencies in public service delivery.

(i)

In 2021, the Government of Malaysia also introduced a new initiative- **Government Cloud**. This is a strategic collaboration between the Government Cloud Service Provider **(CSP)** and four commercial CSP channels.

This initiative empowers public sector agencies in Malaysia to readily adopt technologies such as data analytics, AI and blockchain, helping them achieve the targets outlined in the Malaysia Digital Economy Blueprint **(MyDigital)**. Furthermore, it aligns with the global **Cloud First Strategy,** i.e. prioritising cloud services over conventional data services.

(ii)

Data / Privacy

https://lom.agc.gov.my/ilims/upload/portal/akta/LOM/EN/Act%20709%2014%206%202016.pdf (i)

https://www.malaysia.gov.my/portal/content/654 (ii)

The Personal Data Protection Act 2010 **(APDP),** also known as Act 709, is the most consequential data protection law in Malaysia. It covers a range of topics, including:

1. The seven key data protection principles
2. Responsibilities of data handlers
3. Rights of data subjects
4. Functions and powers of the Data Protection Commissioner
5. Inspection, complaints and investigation processes

(i)

The Personal Data Protection Commissioner (**PPDP**) was formed under the APDP Act of 2010. The PPDP sits within the **Ministry of Digital** and is responsible for regulating and processing commercial transactions of personal data by Data Controllers and protecting individuals from the misuse of their data.

There are various divisions and sections within the PPDP e.g. the Registration and Management Section, the Monitoring Division and the International Policy and Relations Section. Further information about their respective functions and duties can be found in the 'About Us' section on the PPDP's website.

Individuals/entities can also register to become Data Users and file complaints of data protection breaches via the PPDP's website.

(ii)

Commentary

Fraud

https://www.bnm.gov.my/-/nfp-launch (i)
https://nfcc.jpm.gov.my/index.php/en/component/content/article/nsrc-info-link?catid=11&Itemid=114 (ii)
https://www.bnm.gov.my/-/nfp-launch (iii)

Whilst there are **no standalone anti-fraud laws** in Malaysia, the various types of fraudulent crimes and their subsequent penalties can be found in the **Penal Code** (most recently amended 2023), otherwise known as **Act 574**.

(i)

The National Scam Response Centre (**NSRC**) sits within Malaysia's National Anti-Financial Crime Centre (**NFCC**) and serves three main functions:

1. Acting as a central coordinating body for financial crime investigations, providing operational support and expert guidance to enforcement agencies
2. Maintaining an intelligence database to facilitate information sharing
3. Actively engaging in financial crime prevention efforts

(ii)

Bank Negra Malaysia launched the National Fraud Portal **(NFP)** to help solidify the NSRC's capabilities in curbing financial scams and fraud. Some of the main features of the NFP include:

1. Automated fund tracing and recovery
2. Effective industry-wide information sharing and collaboration
3. Data-driven mule assessments i.e. better identification, assessment and monitoring processes

(iii)

Sanctions

https://amlcft.bnm.gov.my/sanctions-related-to-tf-pf-and-other-sanctions (i)
https://www.moha.gov.my/index.php/en/senarai-kementerian-dalam-negeri (ii)

Malaysia implements sanctions in line with the United Nations Security Council Resolutions (**UNSCRs**).

The three sanctions lists applicable to asset freezing in Malaysia are as follows:

1. **The 1267 List**, maintained by the 1267 Committee of the UN Security Council
2. **The 1998 List**, maintained by the 1998 Committee of the UN Security Council
3. **Malaysia's domestic sanctions list**, maintained by the Ministry of Home Affairs (cannot currently be searched online)

(i)

Bank Negra Malaysia is the competent authority responsible for implementing **Targeted Financial Sanctions (TFS)** in Malaysia, performing the following functions:

1. maintaining and updating the sanctions databases; and
2. screening the names of customers and any beneficial owners, beneficiaries (new, existing and potential) and related parties against the sanction's lists.

NB: Data available for viewing at www.kyc-data.com

(ii)

Commentary

Terrorism

https://www.kln.gov.my/web/guest/home/-/journal_content/56/10136/6035635 (i)
https://www.moha.gov.my/index.php/en/menu-utama (ii)
https://www.moha.gov.my/images/MyPCVE/index.html#page/10 (iii)

The most significant counter-terrorism law in Malaysia is the **Prevention of Terrorism Act 2015** (**full document not currently available online**).

Malaysia has previously received criticism from the European Parliament regarding its anti-terrorism laws, highlighting concerns over restrictions on freedom of expression. For instance, the Prevention of Terrorism Act allows "*authorities to arrest any person without a warrant if there is reason to believe that there are grounds to justify the holding of an inquiry into the case of a person*." The Malaysian Government responded to these criticisms, highlighting that the law also states, "*no person shall be arrested solely for his political belief or political activity*".

(i)

The Ministry of Home Affairs (**MOHA**) implements various measures to perturb the financing of terrorism, one of which is asset freezing.

(ii)

The **Malaysia Action Plan on Preventing and Countering Violent Extremism 2024-2028** places particular emphasis on tackling the root causes of terrorism and violent extremism.

(iii)

Company Registrar

https://www.ssm.com.my/Pages/Home.aspx (i)
https://www.ssm.com.my/Pages/Quick_Link_backup/e-Search.aspx (ii)

Companies in Malaysia can be registered via the Company Commission of Malaysia / Suruhanjaya Syarikat Malaysia **(SSM)** website.

(i)

The company registrar can be searched via the **e-Search Portal** by entering the company registration type and registration number.

(ii)

Access to Public Information

https://www.pmo.gov.my/2023/09/enactment-of-freedom-of-information-act-approved-in-principle-pm-anwar/

Whilst Malaysia currently **lacks a formal Freedom of Information Law**, the Special Cabinet Committee on National Governance (**JKKTN**) has agreed (in principle) to the implementation of a Freedom of Information Act. The purpose of the act is to establish clear parameters and guidelines.

Other

https://www.malaysia.gov.my/portal/index

The official website of the Government of Malaysia which provides information and links to key government services for citizens and non-citizens.

Posture Rating – Malaysia

The PR value of **6.6** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	9	9	9	8	7	8	2	4	6	2	2

Malaysia has several well-established processes and offers its citizens a range of modern digital services. The assigned value reflects the available information at the time of writing.

NB: **The figure does not reflect the execution of any laws, regulations or processes.**

Mauritius

Commentary

Financial Regulatory Authority

https://www.bom.mu/ (i)
https://www.bom.mu/about-bank/legislations/banking-act-2004 (ii)
https://www.fscmauritius.org/

The Bank of Mauritius **(BOM)** was established in 1967 as the central bank of Mauritius. The BOM is modelled on the UK's Bank of England and was set up with the assistance of senior officers of the Bank of England.

The Bank performs various functions, including:

1. Conducting **monetary policy** and managing the exchange rate
2. **Regulating and supervising** financial institutions e.g. banks, money changers and foreign exchange dealers
3. Managing **foreign exchange** reserves
4. **Consulting the Government** on financial matters
5. Maintaining the Mauritius **Credit Information** Bureau

(i)

The Bank of Mauritius is governed by the **Banking Act of 2004**. Amendments were made to the Act in 2007 and 2010, enabling the Bank to issue **special licences** to banks wishing to carry out any, or all the following activities: banking business, Islamic banking business, private banking business and investment banking business.

(ii)

The Financial Services Commission (**FSC**) is an independent regulatory body, responsible for regulating, monitoring and supervising the conduct of business activities in the financial services sector.

(iii)

The national currency of Mauritius is the **rupee.**

AI Act / Policy

https://treasury.govmu.org/Documents/Strategies/Mauritius%20AI%20Strategy.pdf

The **Mauritius Artificial Intelligence Strategy 2018** seeks to utilise AI to drive growth and productivity and improve the overall quality of life for the citizens of Mauritius.

The strategy focuses on several areas, including:

1. Application of AI in specific sectors, e.g. agriculture, health and public governance
2. Building human capital in the field of AI
3. Establishing a robust regulatory framework to enable the development of AI
4. Fostering a digital ecosystem to nurture AI in Mauritius

https://www.fiumauritius.org/fiu/wp-content/uploads/2024/04/financialintelligenceandantimoneylaunderingact2002110.pdf (i)

https://www.fscmauritius.org/en/aml/amlcft (ii)

The Financial Intelligence and Anti-Money Laundering Act 2002 (**FIAMLA**) is the most consequential AML law in Mauritius.

One of the main features of the Act is the establishment of the **Financial Intelligence Unit (FIU)**, responsible for the "*request, receipt, analysis and dissemination of financial information*", specifically concerning money laundering or the financing of any activities or transactions related to terrorism.

The main functions of FIU include:

1. **Collecting, processing, analysing** and interpreting all information disclosed to it in line with relevant enactments
2. **Informing, advising and cooperating** with investigatory bodies, the Counterterrorism Unit and Registrars
3. Issuing **guidance** to institutions under its supervision
4. **Exchanging information** with overseas financial intelligence units
5. **Contributing to research projects** to help identify the causes of money laundering and terrorist financing

(i)

The Financial Services Commission (**FSC)** also contributes to implementing AML/CTF measures in Mauritius, focussing on activities in the financial services sector and global business (except banking). This includes:

1. Combatting ML and TF through the **exchange of information** with public sector agencies, international organizations, foreign supervisory institutions or law enforcement agencies
2. Regularly **reviewing its AML/CFT regulatory framework** to ensure international best practices are followed
3. Ensuring the proper **dissemination of investor alerts** from international bodies such as the International Organization of Securities Commission (**IOSCO**)

In addition to its national legislative framework, Mauritius is an active member of the Eastern and Southern Africa Anti-Money Laundering Group (**ESAAMLG**), an associate member of **FATF.**

(ii)

Commentary

Bribery

https://nssec.govmu.org/Documents/Legislations/The_Prevention_of%20Corruption%20Act.pdf (i)

https://fcc.mu/about-the-fcc/ (ii)

Mauritius legislates against bribery in the **Prevention of Corruption Act 2002**. This includes:

- **Section 4** – Bribery by a public official
- **Section 5** – Bribery of a public official
- **Section 8** – Bribery of or by a public official to influence the decision of a public body
- **Section 12** – Bribery for procuring contracts (i)

The Financial Crimes Commission (**FCC**) was established in 2023 under the Financial Crimes Commission Act (**FCC Act**), dealing with a broad spectrum of financial crimes, including bribery and corruption.

The FCC has taken over the functions of the Independent Commission Against Corruption (**ICAC**), the Asset Recovery Investigation Division (**ARID**) and the Integrity Reporting Services Agency (**IRSA**), representing a more unified approach to tackling financial crimes.

The FCC website has a designated page for reporting financial crimes which can be done by post, email, phone, online or in person.

(ii)

https://commerce.govmu.org/Pages/Departments/CAU.aspx (i)
https://mauritiusassembly.govmu.org/mauritiusassembly/wp-content/uploads/2023/03/bill0214.pdf (ii)
https://commerce.govmu.org/Pages/Legislations/Acts-and-Regulations.aspx (iii)

The Consumer Affairs Unit (**CAU**) is a specialised unit within the **Ministry of Commerce and Consumer Protection**, responsible for enforcing consumer legislation and providing overall consumer satisfaction and security. Some of their main activities include:

1. **Educating** consumers through direct contact with people and the media
2. Handling consumer **complaints**
3. Ensuring **compliance** with consumer legislation
4. Conducting **surveys and collecting data** to inform recommendations on regulating goods (i)

The **Consumer Protection Bill (2014)** is the most significant consumer protection law in Mauritius, seeking to promote and safeguard the economic and social welfare of consumers through establishing a comprehensive legal framework, providing adequate protection for consumers and ensuring the consumer market is "*accessible, fair, efficient, responsible and sustainable*".

The Bill makes a range of provisions, including:

1. Establishing the **National Consumer Council**, whose main duty is to promote consumer rights.
2. Establishing a **Consumer Protection Tribunal**, who focus on securing expeditious justice for consumers and traders.
3. Requirements of supervising officers to issue **prohibition** or **enforcement notices.**
4. **Prohibiting traders** from charging unfair prices or engaging in **unconscionable** and other prohibited conducts or activities. (ii)

A full list of Mauritius's consumer protection regulations are available on the Ministry of Commerce and Consumer Protection's website. This includes regulations on the control prices of goods and safety requirements. (iii)

Commentary

Cloud Policy

https://dataprotection.govmu.org/Documents/Presentation/Presentation_2017/Confidentiality%20and%20Data%20Sovereignty%20in%20the%20Cloud.pdf (i)

https://mdpa.govmu.org/mdpa/wp-content/uploads/2024/04/DigitalMauritius2030.pdf (ii)

At the time of writing, Mauritius does not have a specific policy or regulation regarding cloud computing. However, the **Data Protection Office** of Mauritius issued a document outlining some recommendations for cloud service providers to ensure compliance with relevant data laws. For example:

1. Calling for service vendors to adopt a 'privacy-by-design' approach
2. Strong encryption made widely available to users
3. Better service level agreements and policies amongst cloud providers (i)

The **Digital Mauritius 2030 Strategic Plan** highlights some ways in which the Government intends to leverage technologies such as Cloud Computing to help transform the country into a high-income, inclusive economy. This includes committing to implementing **'mauricloud'**, a platform designed for document shar-ing, starting with driver's licences and recruitment in the public sector.

(ii)

Data / Privacy

https://dataprotection.govmu.org/Pages/About%20Us/About-the-Office.aspx (i)

https://dataprotection.govmu.org/Pages/The%20Law/Data-Protection-Act-2017.aspx (ii)

The **Data Protection Office** sits within the Ministry of Technology, Communication and Innovations.

The Office is headed by the Data Protection Commissioner, authorised by the Data Protection Act **(DPA)**to ensure compliance with relevant data protection laws. Some of their powers include:

1. Requesting **information**
2. Applying to a Judge in Chambers for a **preservation order**
3. Issuing enforcement **notices**
4. Conducting priority **security checks**

(i)

The **DPA** came into force in Jan 2018, amending the previous Data Protection Act of 2004.

The Mauritius data protection laws now aligns more closely with international standards and is heavily modelled on the **EU's GDPR**.

(ii)

Commentary

Fraud

https://fcc.mu/about-the-fcc/ (i)

https://fcc.mu/financial-crimes-commission-act-2023/ (ii)

In accordance with the Financial Crimes Commission Act 2023 **(FCC Act)**, the **FCC** is the governing body responsible for detecting, investigating and prosecuting a range of financial crimes in Mauritius, including fraud.

(i)

Part III, Sub-Part III – Fraud Offences of the FCC Act outlines the various types of fraudulent offences (and their subsequent penalties). This includes:

- **Section 39** – Fraud by false representation
- **Section 40** – Fraud by failing to disclose information
- **Section 41** – Making or supplying articles for use in fraud offences
- **Section 42** – Fraud by abuse of position
- **Section 44** – Electronic fraud

(ii)

Sanctions

https://www.fiumauritius.org/fiu/?page_id=2317 (i)

The **UN Act of 2019** provides a legal framework for Mauritius to implement targeted financial sanctions. This includes financial sanctions, arms embargo, travel bans, or any other UN measures.

The UN Act also enables Mauritius to declare individuals as a designated party on a **domestic list**, independently of the UN. These decisions are made by authorities empowered under the Act.

Under the domestic regime, the **Secretary of Home Affairs** is obligated to apply for a freezing order against funds/any other assets of the designated party. N.B. This is not a requirement under the UN regime.

Terrorism

https://www.fscmauritius.org/media/1106/the-prevention-of-terrorism-act-2002.pdf (i)

https://www.fscmauritius.org/media/2178/prevention-of-terrorism-special-measures-regulations-2003.pdf (ii)

The **Prevention of Terrorism Act 2002** is the primary counter-terrorism law in Mauritius. The Act makes provisions for the following:

1. Defining what constitutes a terrorist act
2. Measures for prohibiting terrorist activities and its financing
3. Powers of investigative bodies in combatting terrorism i.e. **the Police** and **the FSC**
4. International cooperation, including mutual assistance and extradition
5. Proscription of organizations deemed to be involved in terrorism

(i)

The **Prevention of Terrorism (Special Measures) Regulations 2003** outlines some specific measures implemented by the FSC to prevent the **financing of terrorism** in Mauritius. This includes domestic and international obligations of the Commission and the Central Bank.

(ii)

Commentary

Company Registrar

https://companies.govmu.org/Pages/default.aspx (i)
https://onlinesearch.mns.mu/ (ii)

Sitting within the Ministry of Finance, the **Corporate and Business Registration Department** is a government office responsible for the following functions;

1. Incorporating, registering and striking off companies
2. The registration of documents that must be filed under the Companies Act, 2001
3. The provision of company information to the public
4. The enforcement of compliance with the legal requirements
5. Registration of Businesses
6. Providing an insolvency service
7. Registration of limited partnerships and foundations

(i)

Search tool for performing searches by Company/Partnership name.

(ii)

Access to Public Information

https://data.govmu.org/

The official government **'opendata portal'** provides public sector information on areas such as health, education, agriculture, social welfare and public security.

At present, Mauritius **does not** have any official laws dedicated to granting access to public information.

Other

https://mygov.govmu.org/Pages/Home.aspx

The Government Portal of Mauritius is the official web portal of the Government of Mauritius.

NB. Multiple URLs for Government websites are available, all using the '.org' suffix.

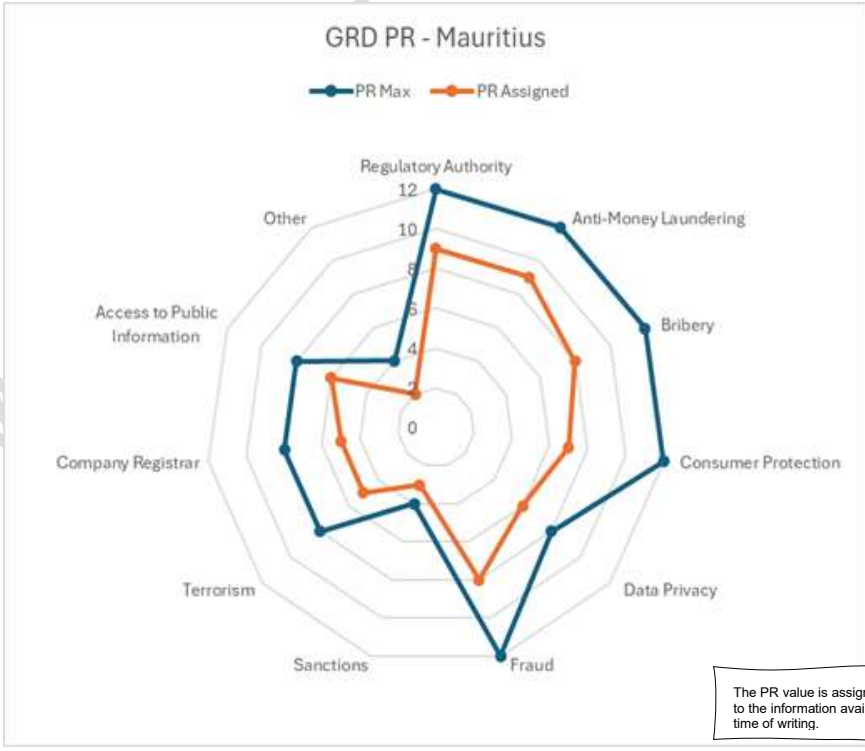
Posture Rating - Mauritius

The PR value of **6.8** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	9	9	8	7	6	8	3	5	5	6	2

Mauritius has several mature and innovative processes to support the regulations and laws required to meet its domain obligations. However, we did observe, many digital channels required updating e.g. the home page of the government website was last updated in 2019.

NB: **The figure does not reflect the execution of any processes, laws or regulations**.



Mexico – The United Mexican States

Commentary

Financial Regulatory Authority

https://www.banxico.org.mx/indexen.html (i)

https://www.banxico.org.mx/getting-to-know-banco-de-mexico/d/%7B5A48EB85-8081-0A27-9205-9D24FC388400%7D.pdf (ii)

https://www.gob.mx/cnbv (iii)

Banco de México, Is the central bank of Mexico and was created on September 1, 1925.

The Bank's fundamental actions and administrative decisions are made exclusively by the **Governing Board**, consisting of 5 members, including the Chair (appointed by the President) and Deputy Governors.

The main powers and duties of the Board include:

1. Authorising banknote issuance and coin minting
2. Resolving issues that involve granting credit to the Federal Government
3. Determining policies and criteria according to which the Bank implements its operations and issues regulations
4. Approving internal bylaws, budgets and labour and hiring regulations
5. Issuing regulations on contracting

(ii)

Mexico's National Banking and Securities Commission - Comisión Nacional Bancaria y de Valores **(CNBV),** is a decentralized body of the Ministry of Finance and Public Credit (**SHCP**), responsible for **authorising, regulating, supervising** and **sanctioning** various sectors/entities within Mexico's financial system.

(iii)

AI Act / Policy

https://www.ania.org.mx/_files/ugd/447d95_c7e6ebee6cf44b38a0d386cc9534f6e5.pdf

Spanish

Mexico's National AI Strategy - **Agenda Nacional Mexicana de Inteligencia Artificial 2030** seeks to create a comprehensive framework that fosters AI innovation, whilst also addressing the ethical concerns associated with AI.

The Strategy has five key objectives:

1. Developing an inclusive governance framework
2. Identifying the use and needs of AI in industry
3. Making medium and long-term recommendations for the Policy Report for public consultation
4. Support Mexico's AI leadership in international forums
5. Promote continuity through changing administrations

Link to the National Alliance of Artificial Intelligence (Mexico).

Anti-Money Laundering

https://www.gob.mx/cms/uploads/attachment/file/196042/SFM_230217.pdf (i)
https://www.gob.mx/cnbv/acciones-y-programas/prevencion-de-lavado-de-dinero-y-financiamiento-al-terrorismo-pld-ft (ii)
https://www.gob.mx/uif/documentos/que-es-la-uif?idiom=es (iii)

There are various financial institutions that help regulate and implement Mexico's AML/CFT regime, including:

1. The **Comisión Nacional Bancaria y de Valores** (**CNBV**) – supervises and regulates a range of financial entities, including banking institutions, brokerage firms, credit unions and exchange houses
2. **The Attorney General's Office** (**PGR**) – investigates and prosecutes money laundering and terrorist financing offences
3. **The Financial Intelligence Unit** (**UIF**) – analyses information from AML/CFT reports, requests relevant information from financial entities, drafts regulations and notifies financial supervisors over non-compliance on reporting activities
4. **The Ministry of Finance and Public Credit** (**SHCP**) – supervises the adequate compliance of financial and non-financial entities with their AML/CFT obligations

(i)

The overall mission of the **CNBV** is to supervise financial institutions, ensuring they meet their AML/CFT obligations, thus promoting greater compliance on a national level. More information about the CNBV's activities and composition is available on its website.

(ii)

Mexico is also committed to fulfilling the **FATF's forty recommendations**. An assessment conducted in 2017 showed that the UIF was **mostly compliant** with these recommendations.

(iii)

Commentary

Bribery

https://www.sna.org.mx/ (i)
https://www.sesna.gob.mx/politica-nacional-anticorrupcion/ (ii)
https://www.oecd.org/en/topics/sub-issues/fighting-foreign-bribery/mexico-country-monitoring.html (iii)

Spanish

The National Anti-Corruption System – Sistema Nacional Anticorrupcion **(SNA)** is a government entity, comprised of several committees at both a state and national level, coordinating efforts to help **prevent, detect and punish corruption and bribery** offences.

(i)

One of the main duties of the SNA is to develop Mexico's anti-corruption policies and regulations. The most recent **National Anti-Corruption Policy** was issued in 2020 and identifies four key objectives:

1. Combatting corruption and impunity
2. Combatting arbitrariness and abuse of power
3. Promoting improvements in the management of public-government contact points
4. Involving society and the private sector

(ii)

Mexico is a Party to the **OECD Anti-Bribery Convention** and as such, is subject to rigorous peer-review and monitoring by the **OECD Working Group on Bribery.**

(ii)

Consumer Protection

https://www.profeco.gob.mx/juridico/pdf/l_lfpc_06062006_ingles.pdf (i)
https://www.gob.mx/profeco/que-hacemos (ii)
https://www.gob.mx/profeco/acciones-y-programas/servicios (ii)

The most consequential consumer protection law in Mexico is the **Federal Consumer Protection Law 1976 (LFPC).** The Law covers a range of areas, including:

1. Powers and duties of relevant authorities in relation to consumer protection
2. Regulatory requirements for information and advertising, promotions and offers, services etc.
3. Warranties for goods and services
4. Penalties for those in violation of the Law
5. Surveillance and verification

The activities of PRI are closely monitored by the **Federal Consumer Attorney**, appointed by the President of Mexico. Their functions include legally representing Consumer Protection Federal Agency **(PROFECO) and** shaping polices to ensure the smooth organization and operation of the Agency.

(i)

PROFECO**,** a decentralised government agency, was established in accordance with the Consumer Protection Law of 1976 (**LFPC**), serving to promote and protect the rights of consumers.

Some of their main powers as specified by the Law include:

1. Representing consumers either individually or collectively, before jurisdictional and administrative authorities and before suppliers
2. Carrying out analysis and research on matters pertaining to consumer protection
3. Providing advisory services to consumers and suppliers

(ii)

PROFECO are involved in a range of programmes and action plans in relation to consumer protection. Information about the services offered and how to contact each **department within the agency** is available on PROFECO's website. Some of the key areas include:

1. Education and Outreach
2. Consumer Defence Offices
3. The Office of the Assistant Attorney General for Services
4. The Office of the Assistant Attorney General for Telecommunications

(iii)

Cloud Policy

https://embamex.sre.gob.mx/hungria/images/stories/docs/nds.pdf

Mexico's **National Digital Strategy** aims to achieve the goal of a *'Digital Mexico'* through the adoption of Information Communication Technologies (ICTs) to maximise economic, social and political impact. The **National Digital Strategy Coordination Office of the President's Office** is responsible for enforcing the strategy and ensuring its objectives are achieved.

Cloud computing is a key focus area of the Strategy, highlighting the need to prioritise cloud computing in the Federal Public Administration**.** Furthermore, it outlines a plan for creating **data distribution centres** to optimise network use and ensure that there's robust infrastructure in place to facilitate cloud services.

Commentary

Data / Privacy

https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf (i)
https://micrositios.inai.org.mx/gobiernoabierto/en/?page_id=773 (ii)
https://home.inai.org.mx/?page_id=3395 (iii)

The main data protection law governing Mexico is the Federal Law for the Protection of Personal Data Held by Private Parties - **Ley Federal de Protección de Datos Personales en Posesión de los Particulares**.

The Law makes provisions for the following areas:

1. The principles of personal data protection
2. Rights of individuals i.e. the right to access, rectify, cancel or oppose the processing of their personal data
3. Restrictions on data transfers to third parties
4. Privacy notice requirements
5. Powers of relevant enforcement authorities (i)

As stipulated in the Federal Law, the **National Institute for Transparency, Access to Information and Personal Data Protection (INAI)** is the main authority responsible for enforcing the Data Protection Law in Mexico. Some of their main functions include:

1. Ensuring compliance with Federal Law for both public sector and private entities.
2. Monitoring activities of organizations involved in data processing and issuing guidance on data protection best practices.
3. Protecting individual rights by investigating and handling data breach complaints.
4. Raising awareness and educating the public about their data protection rights and the importance of data privacy.

(ii)

The various types of **data protection complaint forms** (the public or private sector) are available to download from **INAI website**. The INAI also has a 24-hour **online support desk/chatbot function** to support data protection queries.

(iii)

Fraud

https://www.sna.org.mx/wp-content/uploads/2022/01/CPF_NOV_2021.pdf (i)
https://mexicocity.cdmx.gob.mx/e/basics-for-mexico-city-travel/filing-consumer-complaints-mexico/ (ii)

The **Federal Penal Code** criminalises fraud in its various forms. General fraud provisions are outlined in **Articles 388-389**.

(i)

PROFECO is responsible for handling consumer complaints regarding suspected fraud or business dishonesty. Their service is available to Mexican citizens and foreign nationals.

(ii)

Commentary

Sanctions

https://www.diputados.gob.mx/LeyesBiblio/pdf/63.pdf (i)
https://sanciones.cnbv.gob.mx (ii)

Mexico does not have its own autonomous sanctions regime. However, as a member of the UN, it is legally obliged to comply with the resolutions adopted by the United Nations Security Council (**UNSC**).

The Ministry of Foreign Affairs (**SRE**) is the main body responsible for implementing Mexico's pecuniary sanctions, as stipulated in the **Law to Protect Commerce and Investments from Foreign Laws that Contravene International Law**.

(i)

The CNBV is also authorised to impose sanctions on financial institutions. The list of **CNBV sanctioned entities** can be viewed via its website.

(ii)

Terrorism

https://fgr.org.mx/ (i)
https://www.gob.mx/uif/documentos/que-es-la-uif?idiom=es (ii)
https://www.oas.org/ext/en/main/oas/our-structure/agencies-and-entities/cicte-committee (iii)

Some of the key institutions involved in countering terrorism in Mexico are as follows:

1. The **Attorney General's Office (FGR)** – investigates crimes and seeks to reduce insecurity. (i)
2. The **Financial Intelligence Unit (UIF)** – focussed on preventing and combatting the financing of terrorism. (ii)

Mexico also participates in counter-terrorism measures on an international level, being a Party to the Inter-American Committee Against Terrorism (**CICTE**) and the Financial Action Task Force of Latin America (**GIFILAT**).

(iii)

Company Registrar

Mexico has thirty-one states; each of these states maintains a Public Registry of Property and Commerce **(Registro Público de la Propiedad y de Comercio**) located in its major cities.

There is no national commercial registry for companies in Mexico, Thus, searches for an entity's records are conducted on a local basis and usually, in person.

Commentary

Access to Public Information

https://www.dof.gob.mx/nota_detalle.php?codigo=5391143&fecha=04/05/2015 (i)

https://www.plataformadetransparencia.org.mx/Inicio (ii)

The General Law on Transparency and Access to Public Information establishes the "*principles, general bases and procedures*" to guarantee individuals the right to access public information.

The Law outlines the **requirements for government entities** to publish any relevant information on their websites, making it easily accessible to the public. It also outlines certain **types of information that are exempt** from the provisions of the Law e.g., information related to national security, privacy and ongoing investigations.

(i)

The National Transparency Platform (**Plataforma Nacional de Transparencia**) is an online portal which allows the public of Mexico to do the following:

1. Access information that public institutions are legally obliged to publish
2. Request information about their personal data from different public institutions
3. File a complaint if unsatisfied with the response (online chatbot function also available)

(ii)

Other

https://www.gob.mx/presidencia/ (i)

https://www.gob.mx/ (Ii)

Spanish

The official website for the President of the Mexican Republic.

(i)

The portal for all government ministries and links to several non-government websites.

(ii)

Posture Rating – Mexico

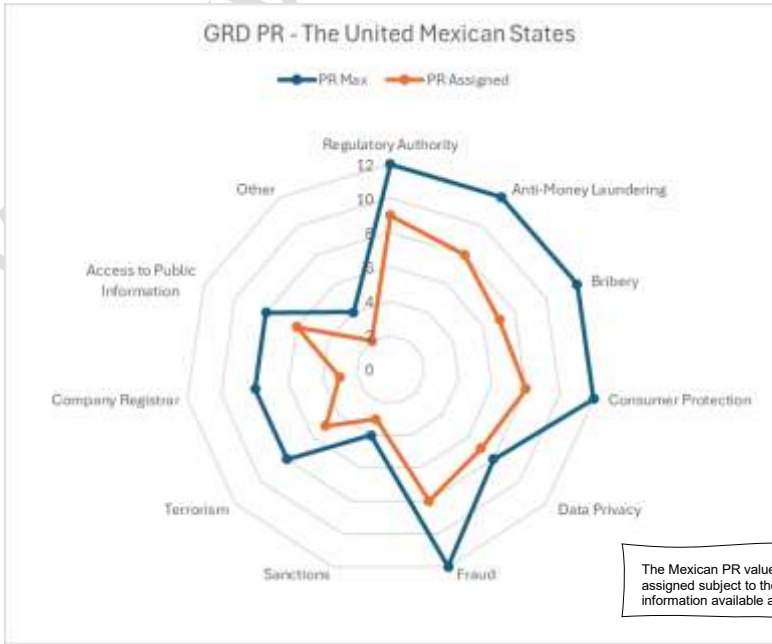
The PR value of **6.6** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	9	8	7	8	7	8	3	5	3	6	2

Mexico has several mature processes that support the regulation and laws for which its obligations for the domains are supported.

Many of the digital services are in the national language and do not offer a translated version. Moreover, Mexico does not have a national company registrar, which is reflected in the assigned value.

NB: **The figure does not reflect the execution of any processes, laws or regulations**.



Netherlands

Commentary

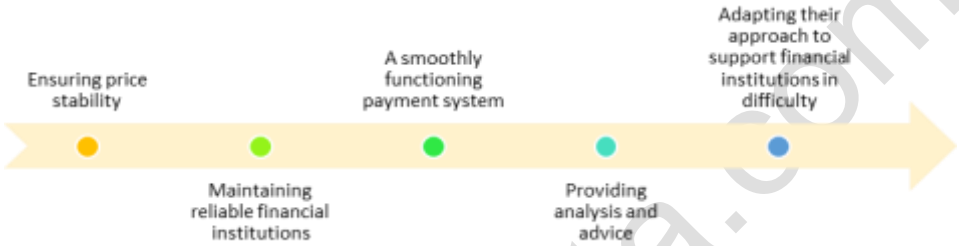
Financial Regulatory Authority

https://www.dnb.nl/en/ (i)

https://www.afm.nl/en/over-de-afm (ii)

De Nederlandsche Bank **(DNB)** is the central bank of the Netherlands and a member of the Eurosystem.

The Bank performs the following functions depicted below.



The DNB has an **independent mandate** for its monetary policy and payment systems. This is also crucial to maintaining the Bank's role as a **special advisor**, regularly reporting to the Dutch ministries of Finance and Social Affairs and Employment about their supervisory activities.

(i)

The Dutch Authority for the Financial Markets **(AFM)** is responsible for supervising the conduct of the financial market sector. This includes savings, investment, insurance, loans, pensions, capital markets, asset management, accountancy and financial reporting.

(ii)

AI Act / Policy

https://www.government.nl/documents/parliamentary-documents/2024/01/17/government-wide-vision-on-generative-ai-of-the-netherlands (i)

https://artificialintelligenceact.eu/the-act/ (ii)

The **Government-wide vision on generative AI** outlines some of the key opportunities and risks associated with generative AI. Furthermore, it addresses relevant **laws, regulations and policies**, setting out a comprehensive framework to ensure the responsible development and use of AI that benefits society.

(i)

As an EU Member State, the Netherlands is also bound by the **EU AI Act 2024.** This means it must adopt a **risk-based approach** to AI regulation, i.e. imposing a gradual scheme of requirements and obligations depending on the level of risk posed to health, safety and fundamental rights.

(ii)

https://www.dnb.nl/en/sector-information/open-book-supervision/laws-and-eu-regulations/anti-money-laundering-and-anti-terrorist-financing-act/#:~:text=The%20Anti%2DMoney%20Laundering%20and,obligations%20arising%20from%20European%20law. (i)

https://wetten.overheid.nl/BWBR0024282/2025-02-04 (ii)

https://www.amlc.nl/over-het-amlc/wat-is-het-amlc/ (iii)

The Anti-Money Laundering and Anti-Terrorist Financing Act (**Wet ter voorkoming van witwassen en financieren van terrorisme – Wwft**) was first issued in 2008 and was then amended in 2018 and 2020 in line with new **EU law** obligations.

The main features of the Act are as follows:

1. **Adopting a risk-based approach** – Institutions are largely free to decide on the level of risk they're willing to take, which then determines the mitigation measures they must implement.
2. **Customer due diligence** – All institutions must carry out customer due diligence measures; the degree of scrutiny is determined by the risk posed by the type of customer, relationship, product or transaction.
3. **Notification duty** – Financial and other institutions specifically listed in the Wwft must report any unusual transactions to the FIU-Netherlands.
4. **Supervision of compliance with the Wwft** – As specified in the Act, the DNB is responsible for supervising Wwft compliance, reviewing the procedures and measures they've implemented to prevent ML/TF.

(i)

Full version of the Act is available on the Overheid.nl website**.**

(ii)

The Anti-Money Laundering Centre **(AMLC)** is the knowledge and expertise centre of the **FIOD**, working to combat money laundering on both a national and international level. Their main activities include:

1. Formulating new money laundering typologies
2. Instigating major money laundering investigations
3. Raising awareness and sharing expertise
4. Analysing data on money laundering and developing relevant tools

(iii)

Commentary

Bribery

https://www.government.nl/ministries/ministry-of-foreign-affairs/contact/reporting-fraud-or-corruption-in-projects-financed-by-ministry-of-foreign-affairs#:~:text=If%20you%20suspect%20fraud%20or,netherlandsworldwide%20for%20visa%20related%20questions. (i)
https://www.rijksrecherche.nl/english (ii)
https://www.government.nl/binaries/government/documenten/leaflets/2023/01/17/honest-business/75246_BuZa_Eerlijk+Zakendoen_EN_v2.pdf (iii)

Individuals who wish to report a case of bribery or corruption may do so by directly emailing the **Corrupt Practices Enterprise Centre (ECM),** sitting within the Dutch Ministry of Foreign Affairs.

(i)

The **Rijksrecherche** is an independent government body, falling under the jurisdiction of the **Public Prosecution Service**. The authority is responsible for investigating alleged cases of criminal conduct **within the government**, including public servants suspected of **fraud or bribery.**

(ii)

Guidance for businesses on preventing and combating bribery and corruption is provided in the publication *'Doing Business Honestly without Corruption'*, a publication issued by the Government of the Netherlands.

As stipulated in the guidance document, bribery is a criminal offence under **Dutch law** in both the **public and private sector**. This also applies to public or private sector employees **abroad.**

(iii)

Commentary

Consumer Protection

http://www.dutchcivillaw.com/civilcodebook066.htm (i)

https://www.acm.nl/en/about-acm/our-organization/the-netherlands-authority-for-consumers-and-markets (ii)

https://business.gov.nl/running-your-business/legal-matters/consumer-law-your-rights-and-obligations-as-a-seller/ (iii)

The Dutch Civil Code is the primary law governing consumer protection in the Netherlands. Specifically, **Section 6.3.3A of Book 6** covers a range of issues concerning **unfair commercial practices**, stipulating the rights and obligations of consumers and sellers. (i)

The Netherlands Authority for Consumers and Markets **(ACM)** is an independent regulatory authority, responsible for competition oversight, sector-specific regulation and the enforcement of consumer protection laws.

The main functions of the AMC include:

1. Offering consumers **free information and advice** about their rights and how to exercise them – consumers can report problems directly to the AMC via the **consumer information portal (ConsuWijzer).**
2. Businesses may **submit tip-offs** about other businesses if they believe they've violated consumer law.
3. Prior to any **merger or acquisition**, businesses must **notify the AMC and apply for a permit** – Applications for permits can be made via their website.
4. Setting **additional rules** for the telecommunications, postal services, healthcare and energy markets to ensure the **affordability, quality and availability** of products and services in these sectors. (ii)

Further information about the **rights and obligations of sellers** in the Netherlands can be found under the ***'Information for Entrepreneurs'*** section of the Government website. (iii)

Cloud Policy

https://www.nederlanddigitaal.nl/documenten/publicaties/2022/11/16/strategie-digitale-economie

The **Dutch Digital Economy Strategy** was released in 2022, outlining clear guidelines for the Government to follow, in conjunction with **EU laws**, to achieve a "*resilient, enterprising, innovative and sustainable digital economy*".

The main elements of the Strategy pertaining to cloud computing include:

1. A commitment to investing publicly and privately in the pre-conditions of cloud applications to stimulate digital innovation and skills
2. An ambition to have at least 75% of SMEs in the Netherlands using advanced digital technologies (such as cloud)
3. Participating in European and international partnerships such as the Important Project of Common European Interest (IPCEI) Cloud Infrastructures and Services

The full version of the Strategy is available online via the Government's website.

Commentary

Data / Privacy

https://www.autoriteitpersoonsgegevens.nl/en/about-the-dutch-dpa/tasks-and-powers-of-the-dutch-dpa (i)
https://www.government.nl/topics/personal-data/data-protection (ii)
https://www.autoriteitpersoonsgegevens.nl/uploads/imported/policy_rules_data_breach_notification_obligation.pdf (iii)

The Dutch **Data Protection Authority (DPA)** is an independent regulator, responsible for supervising the processing of personal data and ensuring entities compliance with relevant laws and regulations.

The DPA is governed by the EU's General Data Protection Regulation (**GDPR**) and the **Dutch Implementation Act** of the GDPR.

Individuals can **report a data breach** or **file a complaint** directly via the DPA's website. (i)

The **Personal Data Protection Act (PDP Act)** regulates what may or may not be done with an individual's personal information. (ii)

The Act was updated in 2016 to include the **data breach notification obligation.** This requires organizations (both in the public and private sector) to immediately notify the DPA as soon as they experience a serious data breach.

Organizations should consult the **'considerations' diagram** on the document's summary page to decide whether it is necessary to notify the DPA. This diagram details the conditions for different breach levels and the corresponding actions. (iii)

Fraud

https://www.fiod.nl/wat-doet-de-fiod/ (i)
https://www.fiod.nl/fraude-melden/ (ii)

The **Dutch Fiscal Information and Investigation Service (FIOD)** is a government body, responsible for investigating and combatting financial and tax fraud. Their main functions include:

1. **Detecting large-scale fraud and organised crime** – the Criminal Intelligence Team (**TCI**) specialises in this, using informants to guide their investigations
2. **Identifying new trends and developments** in society to help shape new polices and advise other investigative services and supervisors
3. **Combatting Money Laundering** by working with the Anti-Money Laundering Centre (**AMLC**). (i)

Online form to **report fraud** via the FIOD's website. (ii)

Sanctions

https://www.government.nl/topics/international-sanctions/policy-international-sanctions

The Netherlands does not have its own domestic sanctions regime. Instead, it implements sanctions agreed upon by the **EU and the UN**.

The **Minister of Foreign Affairs** leads the implementation of international sanctions in the Netherlands. However, they **regularly collaborate** with other ministers for a coordinated approach. For example, the Minister of Finance shares co-responsibility for financial sanctions involving asset-freezing or blocking international transactions.

Commentary

Terrorism

https://www.government.nl/topics/counterterrorism-and-national-security (i)

https://www.government.nl/ministries/ministry-of-justice-and-security/documents/reports/2024/05/17/promote-protect-combat---national-extremism-strategy-for-2024-2029 (ii)

https://www.government.nl/documents/reports/2016/01/15/national-terrorism-list (iii)

The **Ministry of Justice and Security** is the primary government body responsible for implementing counterterrorism measures in the Netherlands. This includes:

1. Imposing **security measures** to protect people and organizations that are at risk of being targeted
2. The **Counterterrorism Alert System** – warns the government and key sectors, e.g. the energy sector, about terrorist threats
3. **Punishing terrorist intent** as well as the offence itself e.g. planning an attack or completing a terrorist training programme (i)

The Ministry of Justice and Security is also responsible for implementing the Government's **National Extremism Strategy 2024 – 2029**. The Strategy is underpinned by three pillars:

1. **Promoting** a resilient and transparent society that can prevent and deter terrorism at its core
2. **Protecting** the democratic legal order and increasing the government's capacity to foil short and long-term efforts by terrorist aggressors
3. **Combatting** the manifestations of extremism (ii)

The **Ministry of Foreign Affairs** maintains the **national sanctions list for terrorism**, containing the names of all individuals and organizations who have been involved in terrorist activities. Pursuant to the **UN Security Council Resolution 1373 (2001),** any entity listed will have their assets frozen and will no longer be able to withdraw money, aiding the prevention of terrorist financing. (iii)

Company Registrar

https://www.kvk.nl/en/ (i)

https://www.kvk.nl/en/search/ (ii)

Netherlands Chamber of Commerce (KVK) is the official registry of all businesses and organizations in the Netherlands. (i)

URL Link for the search capability allowing trade name or KVK number search criteria. (ii)

Access to Public Information

https://business.gov.nl/regulation/freedom-of-information/ (i)

https://wetten.overheid.nl/BWBR0036795/2024-06-19 (ii)

In accordance with the **Open Government Act (Wet Overheid, WOO),** the Government of the Netherlands must make public information accessible to everyone. If an individual is seeking information that has not yet been published, they may file a **WOO request** with the relevant government department.

The request is free and individuals may ask for copies, extracts or summaries. (i)

The **Government Information Reuse Act** mandates that all government information with potential commercial use, such as data on citizens, buildings, or the climate, must be released as **open data**, unless a valid exemption applies. (ii)

Other

https://www.government.nl/ (i)

https://www.overheid.nl/ (ii)

The official government website. (i)

The access point for information about government organizations in the Netherlands. (ii)

Posture Rating Netherlands

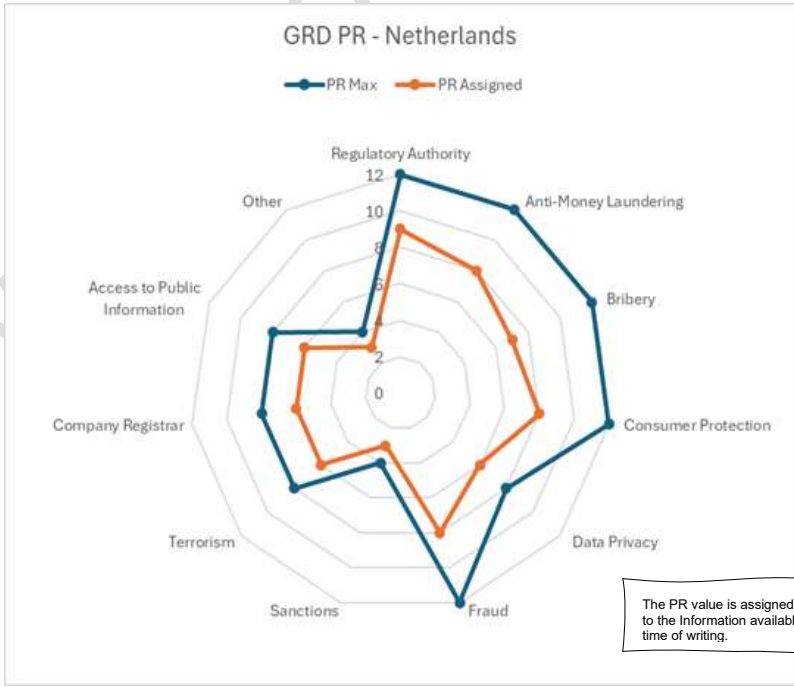
The PR value of **7.0** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	9	8	7	8	6	8	3	6	6	6	3

Netherlands as a member of the European Union, has adopted and extended several EU processes, regulations and laws to support the management of the relevant domains.

The Netherlands has also introduced numerous digital channels to support the domains.

NB: **The figure does not reflect the execution of any processes, laws or regulations**.



New Zealand

Commentary

Financial Regulatory Authority

https://www.rbnz.govt.nz/ (i)
https://www.legislation.govt.nz/act/public/2021/0031/latest/LMS287017.html (ii)
https://www.legislation.govt.nz/act/public/2021/0031/latest/LMS287215.html#LMS287215 (iii)

The Reserve Bank of New Zealand is the central bank of New Zealand; it is also named 'Te Putea Matua' in the Maori language as displayed on the Reserve Bank's website, due to New Zealand's large Eastern Polynesian population.

Established in 1934, its current constitution is outlined under the **Reserve Bank of New Zealand Act 2021,** a legislation outlining the role, purpose and relevant functions of the Bank.

(i)

The Reserve Bank has three main objectives:

1. **Economic**– to maintain price stability
2. **Financial stability**– to promote and protect the stability of New Zealand's financial system
3. **Central Bank**– to act as New Zealand's central regulator

(ii)

The Bank's functions are rooted in maintaining financial stability as well as operating and monitoring monetary policy through the Monetary Policy Committee (**MPC**). The MPC implements policy directed through the Bank's economic objective. There is also an obligation under **Section. 170** of the Act to maintain and deliver a financial stability report which is publicly available via the Bank's website. This may involve updates on New Zealand's financial stability situation or further areas which may be of public interest, as well as research.

The primary functions of the Bank can be allocated as follows (with reference to the 2021 Act);

1. To carry out prudential supervision and act as a prudential regulator, through standard-setting and levelling these standards in accordance with policy
2. Compliance monitoring i.e. it has the capacity to investigate any contravention of its rules and enforce these rules accordingly with the provision that they follow legislative guidelines
3. Take appropriate action when a person or persons has contravened or is likely to contravene the rules

(iii)

The currency of New Zealand is the **New Zealand dollar.**

Commentary

AI Act / Policy

https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23227.html (i)
https://www.data.govt.nz/toolkit/data-ethics/government-algorithm-transparency-and-accountability/algorithm-charter/ (ii)
https://www.digital.govt.nz/standards-and-guidance/technology-and-architecture/artificial-intelligence/public-service-artificial-intelligence-framework (iii)

There are no current laws which relate directly to Artificial intelligence (AI) in New Zealand. However, relevant resources are used to determine how AI is regulated.
The Privacy Act does extent to AI and its enshrined principles are used to provide guidance on regulation; the **Privacy Act 2020** outlines Information Privacy Principles (**IPP's**) which governs how businesses and organizations can handle, collect, store and use personal data. There are 13 IPP's in total; including Purposes for Collection (Principle 1), Storage and Security of Information (Principle 5) and Provision of Personal Access to and individual's data (Principle 6). (i)

Whilst the Privacy Act 2020 does contain information relating to the storage and use of personal data as well as potential for changes brought on by AI, another resource which could be used would be the '**Algorithm Charter for Aotearoa New Zealand'**. This considers the changes brought on by AI and outlines the work required to regulate emerging technologies.

The commitments relating to the Algorithm Charter of New Zealand are outlined in the URL above, which sets a code of practice as to how risk is managed which include regulating emerging technologies. (ii)

The **Public Service AI Framework** promotes the responsible use of AI technologies across the public service. (iii)

Commentary

Anti-Money Laundering

https://www.legislation.govt.nz/act/public/2009/0035/latest/DLM2353113.html (i)
https://www.fatf-gafi.org/en/countries/detail/New-Zealand.html (ii)
https://aml.dia.govt.nz/AMLReportingEntities/ (iii)
https://www.dia.govt.nz/AML-CFT-Legislation (iv)

The primary piece of legislation governing money laundering in New Zealand is the **Anti Money Laundering and Financing of Terrorism Act 2009**; it is divided into two parts with the first dealing with the preliminaries such as definitions and key terms of the Act and the second focussing on AML/CFT requirements and compliance.

As stipulated in the Act, the main governing bodies responsible overseeing and implementing New Zealand's AML/CFT framework are as follows;

1. The Reserve Bank of New Zealand
2. The Financial Markets Authority
3. The Department for International Affairs (i)

New Zealand also maintains its international reputation by adopting and utilising recommendations issued by the Financial Action Task Force (**FATF**), for which it has been a member since 1991. The corresponding URL which provides information relating to New Zealand's FATF participation, as well as its technical compliance ratings in relevant areas.

New Zealand's AML/CFT framework is subject to review by both the FATF and the Asia Pacific Group on Money Laundering (**APG**). These evaluations involve assessing New Zealand's systems and controls against money laundering and terrorist financing, ensuring the robustness if its AML/CFT regime (reports are accessible via the FATF's website).

(ii)

New Zealand's Department of International Affairs (**DIA**) has an online portal called *'AML Online'* which serves to connect the DIA with businesses. AML Online is primarily used by compliance officers of businesses; however, there is an option to delegate.

(iii)

The DIA also maintains an AML/CFT List of Reporting Entities, which is available on the AML Online website. This list includes the names, New Zealand Business Numbers (NZBNs) and regions of entities supervised by the DIA under the **Anti-Money Laundering and Counter Financing of Terrorism Act 2009.**

(iv)

Bribery

https://www.legislation.govt.nz/act/public/1961/0043/latest/DLM328753.html (i)
https://www.ird.govt.nz/international-tax/business/guidance-on-anti-bribery-laws (ii)

The law relating to corruption and bribery of an official is contained within **Section.5 of the Crimes Act 1961.** N.B. there are other relevant items of legislation which relate to corruption, e.g. those taking place from organised criminal groups.

Section 1 outlines that a public official is liable for a 7-year prison term, whether within New Zealand or elsewhere, if they accept or agree to accept a bribe for himself or herself whether through an act done or omitted by him or herself in their official capacity.

Section 2 also outlines the same sentence for those who wish to bribe someone to influence decisions made in the official capacity of the official.

(i)

Further guidance relating to anti-bribery laws can be found the Inland Revenue website, which includes guidance by New Zealand's MOJ.

(ii)

Commentary

Consumer Protection

https://www.govt.nz/browse/consumer-rights-and-complaints/consumer-laws/ (i)
https://www.consumerprotection.govt.nz/ (ii)

The relevant legislation relating to consumer protection law can be found on the New Zealand Government website.

The website contains a broad spectrum of information regarding consumer rights and the corresponding laws to protect them:

1. Problems with product or services - **Consumer Guarantees Act**
2. Problems with borrowing money or using credit - **Credit Contracts and Consumer Finance Act**
3. Businesses acting in a misleading or unfair way – **Fair Trading Act**
4. Protection of personal information – **Privacy Act**

(i)

There is also a **Consumer Protection Portal** which serves as a publicly available tool to reference consumer protection queries.

(ii)

Cloud Policy

https://dns.govt.nz/standards-and-guidance/technology-and-architecture/cloud-services/cloud-adoption-policy-and-strategy/cabinet-minutes-papers/april-2023-proposals-cloud-first-and-strengthening/

New Zealand's **Cloud First Policy** was implemented in 2012. However, after recognising that the policy was no longer aligned with modern domestic markets, the New Zealand Cabinet undertook a **review in April 2023**, looking to also incorporate te ao Māori perspectives and sustainability principles. One of the key elements outlined in the Cabinet paper was the plan to prioritise the adoption of public cloud services as opposed to traditional IT systems and infrastructure.

The new proposals outlined in the paper are available on New Zealand's Digital Government website.

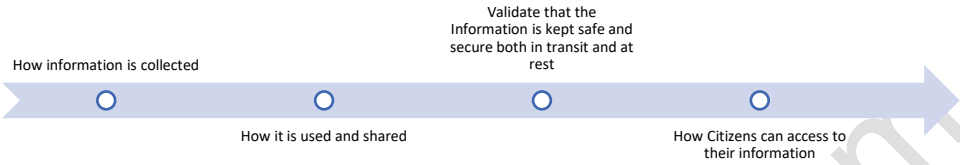
Four direct changes were recommended to the Cabinet involving greater alignment with government priorities, these included;

1. Use Cloud First Policy to reflect societal shifts through incorporating cultural appreciation and sensitivities of indigenous attitudes such as that of Māori to the process and align with government priorities in this manner (previously there had been issues with Māori data sovereignty.
2. Reflect the evolving nature of cloud technology by revoking the IaaS or Infrastructure-as-Service Directive
3. Refresh considerations for security and jurisdictional risk
4. Support and embolden the Government Chief Digital Officer's (GCDO) mandate for cloud digital investment, enabling a transformation of the cloud to be adopted by the public service

There was also a recommendation to move restricted information over time to New Zealand-based data centres where appropriate cloud services exist.

https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html (i)
https://www.privacy.org.nz/ (ii)

The **New Zealand Privacy Act 2020** governs how organizations and businesses can collect, store, use and share information of Citizens and seeks to ensure the following:



The Privacy Act has thirteen foundational privacy principles , as shown below, that govern how businesses and organizations should collect, handle and use personal information.

(i)

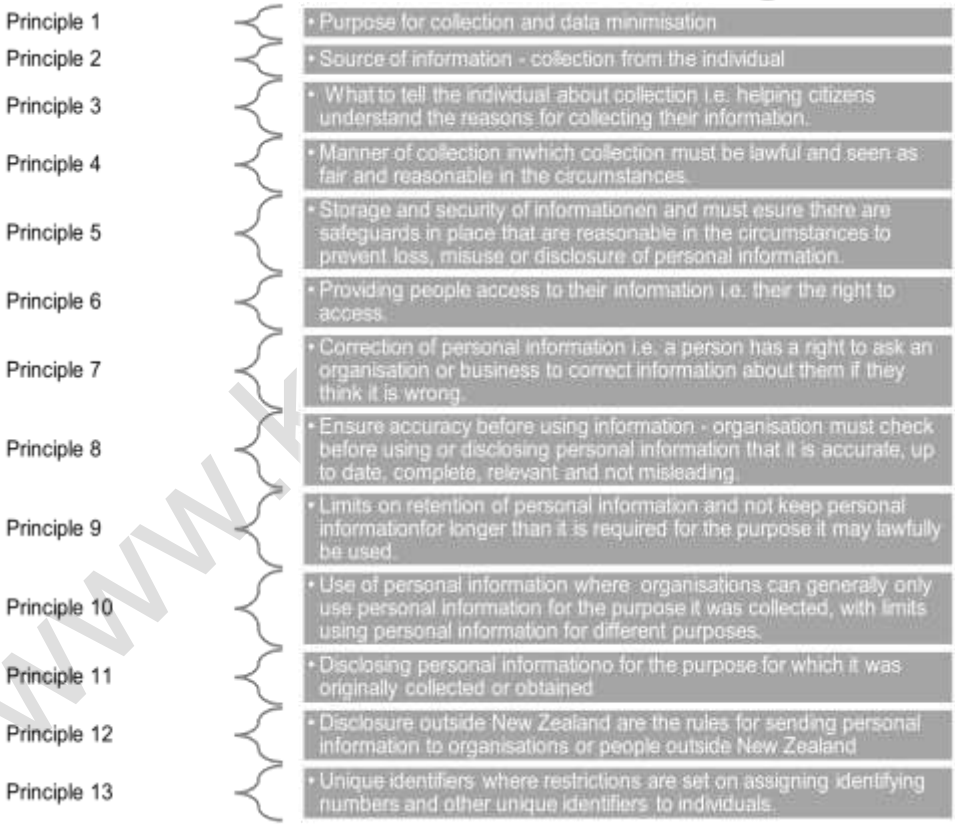


Figure 29 New Zealand Data Privacy Principles

The Office of the Privacy Commissioner (**OPC**) is an Independent Crown Entity. They over-see regulating the Privacy Act 2020 and making sure agencies (businesses and organizations) know what rules they need to follow.

(ii)

Commentary

Fraud

https://www.sfo.govt.nz/

The Serious Fraud Office (**SFO**) is the lead law enforcement agency in New Zealand for investigating and prosecuting serious or complex financial crime, including bribery and corruption. Additionally, they play a key role in preventing financial crime, including bribery and corruption.

The SFO focuses on a relatively small number of **high-profile cases** that have the potential to significantly harm the financial wellbeing of New Zealanders and the economy.

The **NZ Police, Inland Revenue** and the **Financial Markets Authority** are typically responsible for investigating and prosecuting more common, low-profile financial crimes.

Sanctions

https://www.mfat.govt.nz/en/peace-rights-and-security/un-sanctions/ (i)

New Zealand is a member of the UN and therefore is obliged to implement resolutions of the United Nations Security Council regarding sanctions regimes; through reference to the **United Nations Act 1946**. Sanctions information as well as current UN sanctions lists which New Zealand follow and implement can be found on the Ministry for Foreign Affairs and Trade website of New Zealand.

Terrorism

https://www.legislation.govt.nz/act/public/2002/0034/latest/DLM152702.html (i)
https://www.legislation.govt.nz/act/public/2002/0034/latest/DLM151491.html#DLM151490 (ii)

The **New Zealand Terrorism Suppression Act 2002** is one of the primary pieces of legislation in New Zealand governing terrorism. The primary purpose of the Act is to prevent and suppress terrorism at its core, both domestically and internationally. (i)

The Act was amended in November 2023 with the aim of enhancing the existing procedures and ensuring fairness and clarity in relation to the designation of terrorist entities (the full list of incorporated amendments can be viewed via the corresponding URL). (ii)

Company Registrar

https://companies-register.companiesoffice.govt.nz/

The New Zealand Company Office website is where companies in New Zealand can be registered or searched.

Access to Public Information

https://www.legislation.govt.nz/act/public/1982/0156/latest/DLM64785.html

New Zealand's Official Information Act (**OIA**) of 1982 (most recently updated in 2025) allows citizens, permanent residents and anyone residing in New Zealand to request information from government agencies.

Other

https://www.govt.nz/ (i)
https://www.digital.govt.nz/ (ii)

Official website for the government of New Zealand. (i)

Digital.govt.nz aims to be the online source of information, tools and guidance to support digital transformation across the public sector. (ii)

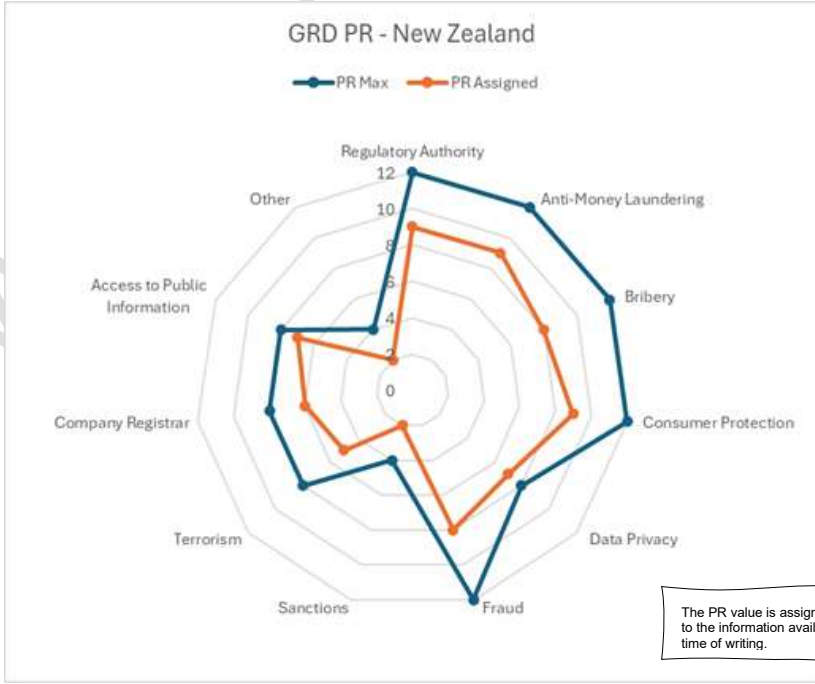
Posture Rating- New Zealand

The PR value of **7.2** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	9	9	8	9	7	8	2	5	6	7	2

New Zealand has a set of mature processes, regulations and laws allowing for compliance of the domains. Many services are supported by digital channels and the PR value reflects the availability of these channels.

NB: **The figure does not reflect the execution of any processes, laws or regulations.**



Federal Republic of Nigeria

Commentary

Financial Regulatory Authority

https://www.cbn.gov.ng (i)
https://www.cbn.gov.ng/OUT/PUBLICATIONS/BSD/2007/CBNACT.PDF (ii)
https://sec.gov.ng/ (iii)

The original mandate of the **Central Bank of Nigeria (CBN)** is derived from the 1958 Act of Parliament.

(i)

The **CBN Act of 2007** of the Federal Republic of Nigeria charges the Bank with the overall control and administration of the monetary and financial sector policies of the Federal Government.

The objectives of the CBN are as follows:

1. Ensure monetary and price stability
2. Issue legal tender currency in Nigeria
3. Maintain external reserves to safeguard the international value of the legal tender currency
4. Promote a sound financial system in Nigeria
5. The Banker and economic and financial advisor of Federal Government. (ii)

The Securities and Exchange Commission Nigeria **(SEC)** is responsible for developing and regulating the capital markets in Nigeria.

The SEC regulates the market through various means, including:

1. **Registration** of securities and market intermediaries
2. Onsite or offsite **inspections**
3. **Surveillance** carried out over exchanges and trading systems
4. Imposing **enforcement actions** for entities that fail to comply with laws and regulations
5. **Rulemaking** to ensure international best practices are maintained

The SEC **develops** the market by collaborating with relevant stakeholders to introduce new products and processes. This includes encouraging investors to participate in activities such as workshops, introducing e-processes and issuing publications.

(iii)

AI Act / Policy

https://fmcide.gov.ng/initiative/nais/ (i)
https://nitda.gov.ng/ncair/ (ii)

The **National Artificial Intelligence Strategy** was published by the Federal Ministry of Communications, Innovation and Digital Economy in 2023.

The Strategy strives to help Nigeria achieve its goals of **job creation, social inclusion and sustainable development.** It does so by building on the existing work of the National Information Technology Development Agency **(NITDA),** expanding on the co-creation approach to engage top AI researchers of Nigerian descent.

(i)

The **National Centre for Artificial Intelligence and Robotics (NCAIR)** is a department within NITDA, dedicated to promoting the research and development of emerging technologies with the aim of transforming the Nigerian digital economy, in line with the **National Digital Economy Policy and Strategy (NDEPS).**

(ii)

https://www.nfiu.gov.ng/images/Downloads/downloads/mlpaamend.pdf (i)
https://www.nfiu.gov.ng/ (ii)
https://www.cbn.gov.ng/Supervision/AML-CFT/ (iii)
https://www.cbn.gov.ng/out/2014/fprd/aml%20act%202013.pdf (iv)

The **Money Laundering (Prohibition) Act of 2011 (ML(PP)A)** was issued by the **Federal Ministry of Justice**, replacing the previous Act of 2004.

(i)

The **Nigerian Financial Intelligence Unit (NFIU)** is an autonomous body, falling under the jurisdiction of the Central Bank of Nigeria. The Unit is responsible for coordinating Nigeria's Anti-Money Laundering, Counter-Terrorist Financing and Counter-Proliferation Financing **(AML/CFT/CPF) framework**.

The core functions of the NFIU include:

1. Handling **suspicious transaction reports** from relevant entities e.g. financial institutions and designated non-financial institutions
2. Receiving threshold-based transaction reports from reporting entities
3. **Analysing information** and utilizing data pulled from local and international databases to enrich reports further
4. **Disseminating intelligence reports** for further investigation by relevant bodies, e.g. law enforcement and anti-corruption agencies

(ii)

The **CNB** also plays a pivotal role in Nigeria's AML/CFT activities, implementing measures to protect the integrity of Nigeria's financial system.

The CNB's main functions in the realm of AML/CFT include:

1. **Mitigating risks** in institutions under their supervision, e.g. commercial banks, finance companies etc.
2. **Adopting a risk-based approach** to AML/CFT supervision of regulated entities
3. **Placing high premiums** on engagements with domestic stakeholders to ensure collective commitment to combatting financial crimes

(iii)

The **CBN (AML/CFT in Banks and Other Financial Institutions in Nigeria) Regulations, 2013** outlines key provisions and regulations on AML/CFT in Nigeria. The Regulation has three main objectives:

1. Provide **AML/CFT** compliance **guidelines**
2. Enables the CBN to **enforce AML/CFT measures** diligently
3. Provides guidance on **Know Your Customer (KYC) measures** to assist financial institutions with the implementation of these regulations

(iv)

Bribery

https://icpc.gov.ng/ (i)

https://www.icpc.gov.ng/wp-content/uploads/downloads/2012/09/CORRUPT-PRACTICES-ACT-2010.pdf (ii)

https://icpc.gov.ng/wp-content/uploads/2024/09/The-African-Union-Convention-on-Preventing-and-Combating-Corruption.pdf (iii)

https://icpc.gov.ng/wp-content/uploads/2024/09/UNcoventionagainscorruption-3.pdf (iv)

The **Independent Corrupt Practices & Other Related Offences Commission (ICPC)** is the regulatory body responsible for fighting corruption in Nigeria. One of their main duties is to educate the public on and against bribery, corruption and related offences. (i)

The ICPC was established according to the **Corrupt Practices and other Related Offences Act 2000**, which outlines in detail their main powers and duties.

The Corrupt Practices Act also establishes specific **provisions for bribery** in its various forms, i.e.:

- **Section 18** – Bribery of a public officer
- **Section 21** – Bribery in relation to auctions
- **Section 22** – Bribery for giving assistance in relation to contracts
- **Section 23** – Obligations of public officers to report bribery transactions

(ii)

On an international level, Nigeria is a state party to the following conventions:

1. The **African Union Convention on Preventing and Combatting Corruption** – seeks to promote a unified approach across African states regarding preventing and criminalising bribery and corruption (iii)
2. The **United Nations Convention Against Corruption** (iv)

Commentary

Consumer Protection

https://fccpc.gov.ng/resources-library/fccpa/# (i)
https://fccpc.gov.ng/about-us/our-mandate/ (ii)

The Federal Competition and Consumer Protection Act, 2018 (**FCCPA**) is the primary law governing consumer protection in Nigeria, seeking to promote *"fair, efficient and competitive markets"* in Nigeria and advocate for the protection of consumer's rights.

The Act establishes two key consumer protection bodies:

1. The Federal Competition and Consumer Protection Commission (**FCCPC**); and
2. The Competition and Consumer Protection Tribunal (**CCPT**)

(i)

The **FCCPC** is the leading consumer protection authority in Nigeria, mandated by the FCCPA.

The FCCPA deploy a range of **regulatory tools** to help safeguard the interests of consumers. These include:

1. **Complaint resolution** – Reports can be made directly via the FCCPC website.
2. **Consumer and Business Education** – Programmes to educate consumers and businesses about their rights and responsibilities.
3. **Strategic communication** – Engaging with the public via available channels to promote compliance with consumer protection laws and regulations.
4. **Legal services** – Services offered include drafting and review, litigation and arbitration management and legal advisory services.
5. **Research and statistics** – Engaging in research on changing/emerging trends in consumer behaviour.

(ii)

Cloud Policy

https://nitda.gov.ng/wp-content/uploads/2020/11/NCCPolicy_New1.pdf

Nigeria Cloud Computing Policy was issued in 2019 by the National Information Technology Development Agency. The main purpose of the strategy is to assist government departments in integrating cloud capabilities quickly and efficiently. To achieve this, the Government is promoting the adoption of a "*Cloud First*" approach amongst Federal Public Institutions (**FPIs**) and SMEs.

Commentary

Data / Privacy

https://cert.gov.ng/ngcert/resources/Nigeria_Data_Protection_Act_2023.pdf (i)
https://ndpc.gov.ng/about-us/ (ii)

Nigeria's Data Protection Act, 2023 (NDP Act) is the primary piece of data protection legislation in Nigeria, seeking to protect individuals' privacy and ensure data is processed in a lawful, fair and transparent manner. Some of the main features of the Act include:

1. Stipulating the rights of data subjects e.g. right to access, correct or withdraw data.
2. Consent requirements for processing data.
3. Security, integrity and confidentiality requirements**,** e.g. impact assessments for data deemed to be high-risk.
4. Processes for **cross-border data transfers.** (i)

The NDPC Act established **Nigeria's Data Protection Commission (NDPC)**, thereby making it responsible for the Act's implementation.

The NDPC offers a range of services, including:

1. Data Protection Compliance Organization (**DCPO**) registration and requirements.
2. Data Controller/Processor registration.
3. Audit filing .
4. Information Portals on licensed DCPOs and Audited firms.

Individuals can report a data breach directly via the NDPC website. The website also offers a free chatbot function to provide additional support and guidance.

(ii)

Fraud

https://icpc.gov.ng/our-role/ (i)
https://www.icpc.gov.ng/wp-content/uploads/downloads/2012/09/CORRUPT-PRACTICES-ACT-2010.pdf (ii)
https://www.efcc.gov.ng/efcc/about-us-new/the-establishment-act (iii)

The **Independent Corrupt Practices and Other Related Offences Commission (ICPC)** is the leading anti-corruption authority in Nigeria. They are responsible for investigating, prosecuting and preventing corruption offences. This includes instructing, advising and assisting officers, agencies or parastatals on how corrupt offences such as fraud may be prevented or eliminated.
(i)

The **Corrupt Practices and other Related Offences Act 2000** criminalises fraud under the following sections:

- **Section 12** – Fraudulent acquisition of property
- **Section 13** – Fraudulent receipt of property (ii)

Another key player in relation to combatting fraud in Nigeria is the **Economic and Financial Crime Commission (EFCC).**

As stipulated in the **Establishment Act 2002** (amended in 2004), the EFCC is mandated to **prevent, investigate, prosecute and penalise** economic and financial crimes. This also involves executing the provisions of other laws and regulations concerning economic and financial crimes, including the **Advance Fee Fraud and Other Fraud Related Offences Act 1995.**

(iii)

Commentary

Sanctions

https://nigsac.gov.ng/Sanctions (i)

https://www.afdb.org/en/projects-operations/debarment-and-sanctions-procedures (ii)

Nigeria's Sanctions Committee (NIGSAC) is responsible for the implementation of the United Nations Security Council Resolutions (UNSCRs).

(i)

Nigeria is a member of the **African Development Bank Group,** and, as such, imposes sanctions on the Bank's list of debarred entities.

Signatories of the Agreement for **Mutual Enforcement of Debarment Decisions** also implement the Bank's sanctions list**.**

(ii)

Terrorism

https://nctc.gov.ng/ova_doc/terrorism-prevention-publication-web/ (ii)

https://nctc.gov.ng/ (i)

The primary counter-terrorism law in Nigeria is the **Terrorism Prevention and Prohibition Act 2022.** Its main objective is to provide a comprehensive legal, regulatory and institutional framework for **detecting, preventing, prohibiting, prosecuting** acts of terrorism and terrorist financing.

Some of the key provisions within the Act include:

1. Defining the powers of relevant law enforcement agencies, including the **Attorney General** and the **National Counter-Terrorism Centre**
2. Implementation of targeted financial sanctions and the powers of the National Sanctions Committee
3. **International cooperation**, i.e. mutual legal assistance, exchange of information and extradition

(i)

The National Counter Terrorism Centre **(NCTC)** was established according to the **Terrorism Prevention Act of 2022** and is designated as the coordinating body for counterterrorism and terrorism financing in Nigeria.

The NCTC performs a range of functions, including:

1. Coordinating counterterrorism **polices, strategies, plans** and support in line with Nigeria's Counter-Terrorism Objectives
2. Facilitating **regional collaboration** in counter-terrorism programmes by partnering with local and international stakeholders
3. Providing **leadership and guidance to institutions involved in counter-terrorism activities**, including the Armed Forces, security, law enforcement and intelligence agencies

Company Registrar

https://www.cac.gov.ng/ (i)

https://search.cac.gov.ng/home (ii)

Companies can be registered via the Corporate Affairs Commission Nigeria **(CAC)**. This includes a step-by-step guide on how to register companies, business names and incorporated trustees.

(i)

The company registrar can be searched using the following URL.

(ii)

Commentary

Access to Public Information

https://foia.justice.gov.ng/resources/downloader.php?filename=Freedom_Of_Information_Act.pdf (i)

https://foia.justice.gov.ng/index.php?option=com_content&view=article&id=11&Itemid=126&lang=en (ii)

The **Freedom of Information Act 2011 (FOIA Act)** makes provisions to ensure public access to public records and information.

(i)

Information on **how to make a FOIA request**, including the specific timelines and processes, can be found on the **FOIA Nigeria website.**

(ii)

Other

https://nass.gov.ng/ (i)

https://services.gov.ng/ (ii)

https://www.cbn.gov.ng/Out/2022/CCD/PSMD%20vision%202025%20EDITED%20FINAL.pdf (iii)

The National Assembly website provides users access to various bills.

(i)

The portal provides citizens residing in Nigeria or abroad with access to digital government services.

(ii)

Nigeria Payments System Vision 2025.

(iii)

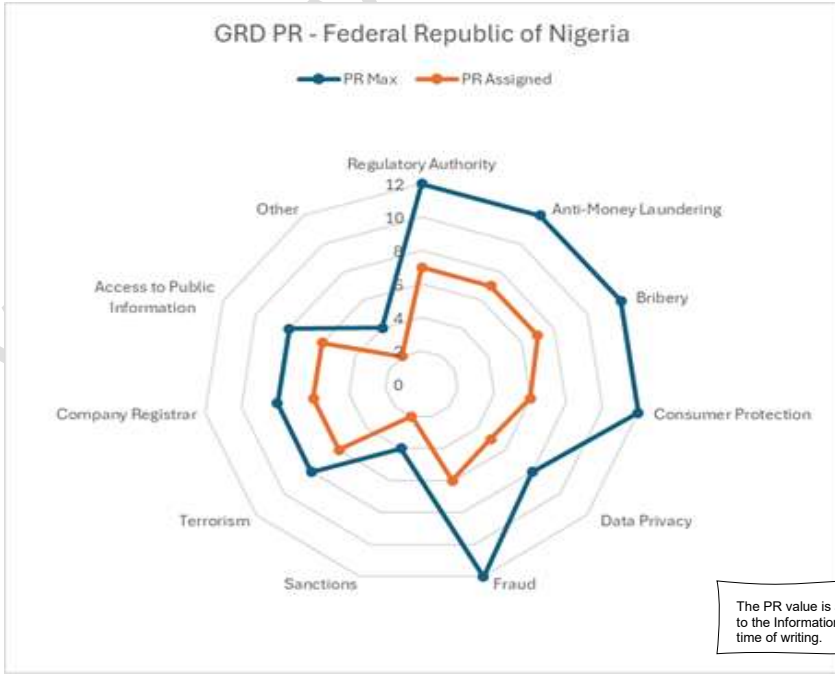
Posture Rating – Nigeria

The PR value of **6.0** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	7	7	7	6	5	6	2	6	6	6	2

Nigeria has defined processes, regulations and laws that allow for its compliance across the domains. Whilst Nigeria is currently in the process of developing its digital channels, we observed several weaknesses regarding their usability, which has been reflected in the assigned value.

NB: **The figure do not reflect the execution of any processes, laws or regulations in Nigeria.**



The Sultanate of Oman

Commentary

Financial Regulatory Authority

https://cbo.gov.om/ (i)

https://cbo.gov.om/Pages/FixedPeg.aspx (ii)

The Central Bank of Oman (**CBO**) was established in December 1974 and is the single integrated regulator for the banking and financial services sector in Oman.

(i)

Due to Oman's highly open economy and overall economic structure, the CBO has chosen to implement a **fixed-peg policy** of the RO to the US Dollar (USD) since 1986. As such, the CBO's monetary policy is centred solely around domestic liquidity management under a fixed exchange rate regime.

(ii)

The national currency of Oman is the **rial** Omani**.**

AI Act / Policy

https://www.mtcit.gov.om/ITAPortal/Data/SiteImgGallery/20223981295/Artificial%20Intelligence%20Systems%20Policy%20v1.0%20(1).pdf

In 2021, the Ministry of Transport, Communications and Information Technology released an official document outlining Oman's **Artificial Intelligence Systems Policy.**

The policy sets out ethical principles and standards for the Omani Government Administrative Units to adhere to, aiming to improve the overall usage of systems and eliminate potential risks. The six policy principles are as follows:

1. **Inclusiveness**- Maximising the benefits of AI for all members of society
2. **Human-centred**- Focus on improving human quality of life
3. **Accountability**- Clear lines of accountability on all AI processes and systems
4. **Fairness**- Ensure appropriate laws are enforced and no human rights are breached
5. **Transparency**- Full access to information regarding the decisions mase by AI systems
6. **Safety**- Compliance with all security procedures and practices

Commentary

Anti-Money Laundering

https://cbo.gov.om/Pages/AntiMoneyLaundering.aspx (i)

https://www.fatf-gafi.org/en/countries/global-network/middle-east-and-north-africa-financial-action-task-force--menafa.html (ii)

On a national level, the primary piece of legislation in Oman in relation to anti-money laundering is the **Royal Decree No. 30/2016,** Promulgating the Law on Combatting Money Laundering.

The law stipulates the powers of each of the regulatory body responsible for enforcing anti-money laundering policies, i.e. the **National Committee for Combatting Money Laundering and the Financing of Terrorism**, the **National Centre for Financial Information** and the **CBO** themselves.

(i)

As a founding member of the **Middle East and North Africa Financial Action Task Force (MENA FATF),** the CBO's anti-money laundering policies are largely shaped by the FATF's recommendations. Some of these include:

1. Enhancement of the role of the financial system in combatting money laundering
2. Customer identification and record keeping
3. Focus on large, unusual and suspect transactions
4. Development of policies, programmes, training and audit and compliance functions

(ii)

Bribery

https://oman.om/docs/default-source/default-document-library/omani-penal-law.pdf?sfvrsn=64250c36_2 (i)
https://www.unodc.org/documents/treaties/UNCAC/CountryVisitFinalReports/2016_07_04_Oman_Final_Country_Report_English.pdf (ii)
https://www.unodc.org/documents/brussels/UN_Convention_Against_Corruption.pdf (iii)

There are currently no standalone legislations against bribery in Oman. Instead, laws against bribery can be found in the **Royal Decree 7/2019, Promulgating the Penal Law (Articles 207-212).** This outlines the definitions of bribery (only covering bribery of public officials) and the penalties in place to help prevent it from occurring.

(i)

Despite being a signatory of the **United Nationals Convention against Corruption (UNAC)**, Oman does not legislate against bribery in the private sector.

(ii)

UNAC stipulates in Article 21 that State Party's should consider adopting legislation against bribery in the private sector, however, does not outline it as a mandatory measure.

(iii)

Consumer Protection

https://oman.om/docs/default-source/default-document-library/consumer-protection-law.pdf?sfvrsn=fab6f8d1_2

The Royal Decree No. 66/2014, To Promulgate the Consumer Protection Law outlines the basic rights of consumers in Oman and highlights obligations of product/service suppliers.

The **Public Authority for Consumer Protection** is the governing body for all matters pertaining to consumer protection.

Commentary

Cloud Policy

https://www.mtcit.gov.om/ITAPortal/Data/SiteImgGallery/20241317542819/Cloud%20First%20Policy.pdf (i)
https://www.moheri.gov.om/userupload/Policy/Cloud%20Governance%20Framework.pdf (ii)

Oman's **Cloud First Policy** was issued by the Ministry of Transport, Communications and Information Technology in 2021. There were several aims behind this publication, some of which include:

1. Ensuring Cloud Computing services are prioritised with regards to decisions surrounding IT services
2. Higher level of efficiency when governing IT resources
3. Protecting the rights of beneficiaries and the quality of services

(i)

Section 5.6 of Oman's **Cloud Governance framework** (**2017)** highlights the various legal implications of adopting cloud services within Oman for both government agencies and cloud service providers themselves. This includes outlining specific laws, regulations and mandates aimed at protecting data and the security of information.

(ii)

Data / Privacy

https://qanoon.om/p/2022/og1429/

In 2022, Oman issued the **Personal Data Protection Law (PDPL),** its first standalone law with regards to data protection and privacy. Some of the key elements of this law are as follows:

1. Clearly defining the **types of data businesses/institutions/government agencies** are obliged to protect e.g. genetic, biometric and health.
2. Outlining instances whereby the **provisions of the law do not apply** e.g. if protecting national security/public interest.
3. Establishing the **duties and powers of the governing body** (the Electronic Defence Centre).
4. Outlining the **rights of personal data holders**, emphasising the need for consent prior to the processing of any data.
5. Stipulating the **obligations of controllers and processors** to ensure appropriate procedures are in place when processing personal data.
6. **Penalties** for those in violation of the law.

Fraud

https://oman.om/docs/default-source/default-document-library/omani-penal-law.pdf?sfvrsn=64250c36_2 (i)
https://cbo.gov.om/sites/assets/Documents/English/Circulars/2017/BM1153.pdf (ii)

Article's 349-355 of the Omani **Penal Law Promulgated by Royal Decree 7/2018** enumerate the specific conditions and circumstances that would lead to an individual/entity being criminally prosecuted for committing fraud.

(i)

Considering growing concerns regarding the rise of fraudulent activities occurring in Oman, the CBO decided to issue a **Fraud Risk Management Framework (FRMF)** in 2017, outlining clear instructions for licensed banks on how to effectively combat and mitigate the risks of fraud. (ii)

Commentary

Sanctions

https://cbo.gov.om/sites/assets/Documents/English/Circulars/2022/Guidelines%20to%20the%20implementation%20of%20Targeted%20Financial%20Sanctions.pdf#search=sanctions%20list

As a United Nations **(UN)** Member State, Oman is obliged to implement targeted financial sanctions on activities related, but not limited to terrorism, terrorist financing and the financing of weapons of mass destruction.

Regulatory measures must be in accordance with the United Nation's Security Council Resolutions **(UNSCR).**

Terrorism

https://www.oman.om/docs/default-source/default-document-library/law-on-combating-money-laundering-and-terrorism-financing.pdf?sfvrsn=7fafb7e3_2 (i)

https://www.un.org/en/ga/sixth/74/int_terrorism/oman_e.pdf (ii)

In 2016, Oman issued the **Law on Combating Money Laundering and Terrorist Financing.** In accordance with this law, the supervisory authorities responsible for governing activities relating to terrorism are as follows:

- the Ministry of Justice;
- the Ministry of Commerce and Industry;
- the Ministry of Housing;
- the Ministry of Social Development;
- the Central Bank of Oman;
- the Capital Market Authority and
- any other party designated by decision of the National Committee for Combatting Money Laundering and Terrorist Financing.

(i)

As a member of the UN, Oman is committed to the goals and **Charter of the United Nations** to maintain international peace and security. As such, they have imposed various measures to support the eradication of terrorism. These include but are not limited to:

1. Prohibiting travel by citizens to conflict zones to counteract the spread of extremist ideologies
2. Creation of several major counter-terrorism bodies e.g. the National Counter-Terrorism Committee and the National Committee to Combat Money Laundering and the Financing of Terrorism
3. International cooperation with other UN Member States and other neighbouring states

The exhaustive list can be found on the official UN website.

(ii)

Company Registrar

https://www.business.gov.om/portal/searchEstablishments?execution=e2s1

The Commercial Registration (**CR**) number serves as the exclusive identifying code for all Omani legal companies.

This public Government service allows for the search of commercial registrations' information in Oman.

Commentary

Access to Public Information

https://www.mtcit.gov.om/ITAPortal/Pages/Page.aspx?NID=1371&PID=5439&LID=278

The **National Centre for Statistics** is responsible for ensuring access to open data relating to the Sultanate of Oman.

The link to access the Government E-Portal for open data can be found on the Ministry of Transport, Communications and Information Technology's official website.

Other

https://www.omaninfo.om/english (i)

https://www.omaninfo.om/module.php?m=pages-showpage&CatID=204&ID=800 (ii)

The official website for the Sultanate of Oman.

(i)

The Council of Ministers assists His Majesty the Sultan in drawing up the general policy of the Sultan.

(ii)

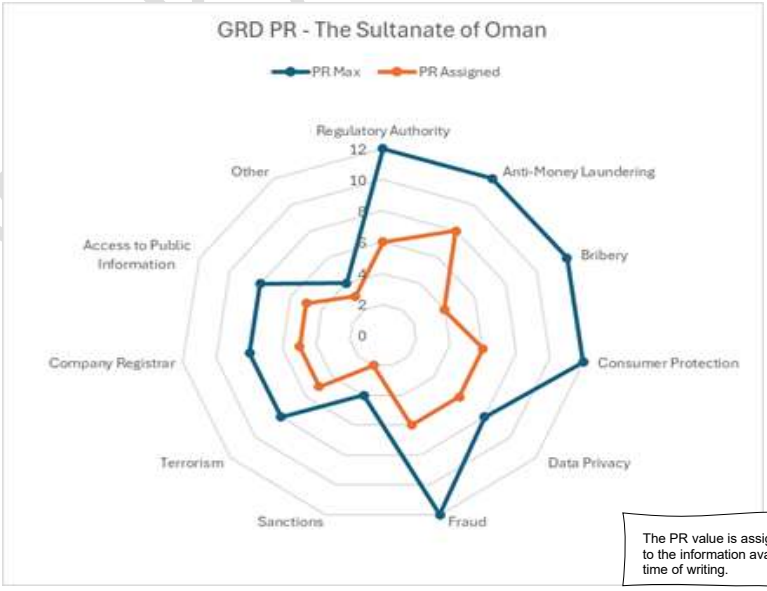
Posture Rating - Oman

The PR value of **5.6** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	6	8	4	6	6	6	2	5	5	5	3

Oman has a defined set of processes, regulations and laws allowing for compliance of the domains. Nevertheless, the digital representation of all sectors is not equally strong. While the Central Bank of Oman offers some effective digital channels, significant issues were identified in bribery. Furthermore, the policy of pegging the Omani rial to the US dollar presents limitations on the range of services offered and these factors collectively contribute to the overall rating.

NB: **The figure does not reflect the execution of any processes, laws or regulations**.



Peoples Republic of China

Commentary

Financial Regulatory Authority

http://www.pbc.gov.cn/english/index.html (i)
https://www.nfra.gov.cn/en/view/pages/index/index.html (ii)
http://www.csrc.gov.cn/csrc/c100002/common_zcnr.shtml (iii)

The People's Bank of China (**PBC**) is China's Central Bank. Founded in 1948, it manages the nation's monetary policy and financial stability, serving as the exclusive issuer of the **Chinese yuan** (also known as Renminbi).

The PBC performs a range of functions, including:

1. Drafting and enforcing relevant **laws, rules and regulations** that are related to fulfilling its functions
2. Formulating and implementing **monetary policy**
3. **Issuing the Renminbi** and administering its circulation
4. **Regulating financial markets**, including the inter-bank lending market, the inter-bank bond market, the foreign exchange market and the gold market
5. Preventing and mitigating systemic financial risks to **safeguard financial stability**
6. **Managing the State treasury** as fiscal agent

(i)

The National Financial Regulatory Administration (**NFRA**) was officially established in 2023, falling under the jurisdiction of the **State Council of the People's Republic of China**.

The NFRA is responsible for regulating China's financial sector (except for the securities sector), taking over several functions from the PBC and the Chinese Securities Regulatory Commission (**CSRC**).

Some of the NFRA's main duties include:

1. Conducting unified **supervision** and **regulation** of the financial sector
2. Carrying out systematic **research**, drafting relevant laws and **regulations** on financial institutions and banks and putting forward recommendations for reform
3. Establishing a sound system and researching major issues concerning the **protection** of financial consumer's rights and interests
4. Preparing regulatory data **statements** for financial entities under their supervision

(ii)

The CSRC also sits directly under the State Council of the People's Republic of China. Their main purpose is to implement the principles, polices and decision-making arrangements of the **CPC Central Committee**. This includes strengthening supervision and control of the capital market and formulating regulatory rules for the securities and futures fund market.

(iii)

Commentary

AI Act / Policy

https://www.mfa.gov.cn/eng/wjbzhd/202409/t20240927_11498465.html

The Ministry of Foreign Affairs issued China's 'AI Capacity-Building Action Plan for Good and for All', a strategy aimed at delivering the following :

Figure 30 China's AI Capacity-Building Action Plan for Good and for All Objectives

Anti-Money Laundering

http://camlmac.pbc.gov.cn/fxqzhongxin/3558093/3558111/3561752/index.html (i)
http://www.pbc.gov.cn/en/3688241/3688777/3688780/3819925/index.html (ii)
https://apgml.org/members-and-observers/members/details.aspx?m=cb329e3b-4dab-46af-89b3-bee66576271b (iii)

The **Anti-Money Laundering Law of the People's Republic of China** is the primary law governing money laundering in China.

The Law covers the following areas:

1. **Supervision and regulation** on anti-money laundering – this includes outlining the powers and duties of the Competent Authority in charge of anti-money laundering affairs under the State Council.
2. **Anti-money laundering obligations for the financial institutions** – for example, the requirement for all financial institutions to establish a customer identification programme.
3. **Anti-money laundering investigations** – the PBC and its dispatched institutions are authorised to conduct investigations and verify any suspicious transactions.
4. **International cooperation against money laundering** – the PBC represents the Chinese government on the international stage, under the supervision of the State Council, exchanging information or materials concerning AML with overseas AML authorities (i)

Under the Law of the People's Republic of China on the People's Bank of China, the PBC is the Competent Authority responsible for supervising financial institutions on matters concerning money laundering.

The China Anti-Money Laundering Monitoring and Analysis Centre (**CAMLMAC**) sits within the PBC, established in 2004 as an administrative Financial Intelligence Unit (FIU). Their main purpose is to support law enforcement agencies in tackling money laundering and other related crimes by *collecting, analysing and disseminating* financial intelligence. (ii)

Alongside its domestic AML regulatory framework, China is also a founding member of the Asia/Pacific Group on Money Laundering (**APG**), which seeks to "ensure the adoption, implementation and enforcement of internationally accepted anti-money laundering and counter-terrorist financing standards as set out in the FATF Forty Recommendations". Additionally, China has signed and ratified all UN Conventions concerning money laundering and became a member of the FATF in 2007. (iii)

Commentary

Bribery

http://en.npc.gov.cn.cdurl.cn/2020-12/26/c_921604_13.htm (i)
http://en.moj.gov.cn/2024-03/04/c_967158.htm (ii)

Bribery is criminalised in China, as stipulated in **Chapter VIII – *"Crimes of Embezzlement and Bribery"*** the Criminal Law of the People's Republic of China.

Articles 385-393 of the Criminal Law cover a range of bribery offences, including:

1. Soliciting or accepting bribes to or from **State Functionaries**
2. Soliciting or accepting bribes in the context of **business** or exchanges between **private entities and individuals** (i)

In 2023, the Standing Committee of the National People's Congress adopted some new amendments to the Criminal Law concerning bribery. The amendments aim to expand the scope of existing bribery laws in China, ensuring more stringent penalties are enforced to help prevent and combat bribery offences. The main features of the amendments are as follows:

1. Adding **seven new types of bribery offence,** e.g., repeatedly offering bribes or offering bribes to multiple people.
2. Enforcing **more severe penalties** on entities offering bribes to those involved in the country's **key work areas**, e.g., organization and personnel affairs, discipline and law enforcement, justice, food and medicine and education. (ii)

Consumer Protection

http://www.pbc.gov.cn/en/3688241/3688711/3688714/index.html (i)
http://www.npc.gov.cn/zgrdw/englishnpc/Law/2007-12/12/content_1383812.htm (ii)
https://english.www.gov.cn/policies/latestreleases/202403/19/content_WS65f974b2c6d0868f4e8e53d1.html (ii)

The PBC established the **Financial Consumer Protection Bureau** in 2012, responsible for ensuring financial inclusion and financial consumer protection. Some of their main duties include:

1. **Conducting research** on major issues pertaining to financial consumer protection in China
2. **Formulating** drafts of polices and regulations
3. **Monitoring** the risks of cross-sector financial instruments (i)

The primary law governing consumer protection in China is the **Law of the People's Republic of China on the Protection of Consumer Rights and Interests**. This outlines:

1. The obligations of sellers/business operators;
2. The rights of consumers; and
3. The duties of relevant state organs and consumer associations in implementing consumer protection measures. (ii)

In **March 2024**, refined regulations were introduced concerning the implementation of the nation's law on the protection of consumer rights and interests. Some of the key changes include:

1. Standardised consumer **complaints and compensation** claims
2. Refined provisions regarding **online consumption and operators' obligations**
3. Calling on government departments to **strengthen guidance** on the protection of consumer's rights and interests, increase supervision, inspection, law enforcement and investigations (ii)

Commentary

Cloud Policy

https://english.www.gov.cn/policies/latest_releases/2016/12/27/content_281475526646686.htm

China's 14th Five-Year Plan on Informatization (2021-2025) incorporates emerging technologies such as cloud computing as part of one of its key initiatives to *"unlock the potential of big data, build China's strength in cyberspace, accelerate the development of a digital economy, a digital society and a digital government*".

Some of the key elements of the strategy involving the use of cloud computing include:

1. Integrated R&D of general-purpose processors, cloud computing systems and core software technologies to drive innovation and application services
2. Digital transformation and development of traditional industries using cloud-based solutions and AI initiatives
3. Building cloud platforms and data centre systems to promote cloud migration of government systems

Data / Privacy

http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm (i)
https://www.cac.gov.cn/wxzw/sjzl/A093708index_1.htm (ii)

The **Personal Information Protection Law of the People's Republic of China (PIPL)** was enacted at the 30th Meeting of the Standing Committee of the Thirteenth National People's Congress in August 2021.

The law covers a range of areas, including:

1. Legal bases for personal information processing
2. Rights of individuals
3. Specific rules for highly sensitive personal information
4. Cross-border data transfers
5. Government use of personal information

(i)

There is no singular authority dedicated to data protection in China. Instead, the **Cyberspace Administration of China (CAC)** takes responsibility for the overall planning and coordination of data protection regulations in China.

(ii)

Using a VPN in China is technically legal. However, all VPN services operating in China must be approved by the Chinese Communist Party (**CCP**). Most VPN providers in China are obliged to log user data.

The Chinese government implemented the Great Firewall in the early 2000s to control access to foreign websites and online services for its citizens.

Commentary

Fraud

http://en.npc.gov.cn.cdurl.cn/2020-12/26/c_921604_13.htm (i)
http://nl.china-embassy.gov.cn/eng/ls/202303/t20230321_11045403.htm (ii)

Fraud is criminalised in China pursuant to the **Criminal Law of the People's Republic of China,** under the following articles:

- **Article 269** – Fraud of someone else's property
- **Article 287** – Online financial fraud
- **Article 287a** – Setting up websites or online communication groups to commit fraud
- **Article 319** – Fraud in the context of labour, exports, commerce and trade
- **Article 382** – Fraud committed by a State Functionary (i)

China's **Anti-telecom and Online Fraud Law** is a key piece of legislation concerning combatting fraud in China. As stipulated in the law, the relevant **public security organs** shall **lead on anti-fraud measures** in their respective departments. The key departments include finance, telecommunications, cyberspace administration and market regulation. (ii)

Sanctions

China adopts the United Nations Sanction-Related Resolutions. However, China also enacted several laws and regulations in 2019 and 2021, respectively, to establish its own sanctions against foreign persons.

The Ministry of Foreign Affairs (**MFA**) is primarily responsible for administering UN sanctions through administrative notices and various regulatory authorities. This includes authorities such as: the Ministry of Commerce (MOFCOM), the People's Bank of China (the central bank), the China Banking and Insurance Regulatory Commission, the China Securities Regulatory Commission, the Ministry of Transport, the General Customs of China and the Ministry of Public Security, all of which enforce sanctions programmes within their respective authorities.

As to China's own counter-sanctions measures, the **MFA** and **MOFCOM** are the primary authorities responsible for administration and enforcement. Other regulatory authorities also participate in implementing countermeasures such as assets freezes and entry denials.

Commentary

Terrorism

http://english.scio.gov.cn/node_9006693.html

China's Legal Framework and Measures for Counterterrorism, 2024 is comprised of a range of criminal laws and regulations, including the National Security Law and administrative regulations.

The main features of the publication are as follows:

1. **Improving China's legal framework** for counterterrorism – this includes strengthening international cooperation by ratifying several UN conventions and instruments
2. Making clear provisions for the **determination and punishment of terrorist activities** – distinguishing between administrative violations and criminal acts based on the degree of harm caused
3. **Unifying approach to fighting terrorism** across relevant law enforcement bodies – powers of law enforcement and judicial agencies subject to monitoring by the Chinese People's Political Consultative Conference (**CPPCC**)
4. Making clear provisions for protecting human rights in the context of counterterrorism practices – using human rights as the guiding principle when developing legal framework
5. **Effective protection of people's safety and national security,** e.g. greater sense of public security and assistance for victims of terrorism

Company Registrar

https://www.gsxt.gov.cn/index.html (i)
https://www.registrationchina.com/ (ii)
https://www.registrationchina.com/china-company-search/ (iii)

The **National Enterprise Credit Information Publicity System** allows viewing of the legal status of a company and is administered by the State Administration for Marketing Regulation.

(i)

Companies in China can be registered via the **GWBMA website.** The GWBMA provides company registration and business consulting services, offering comprehensive guidelines for businesses throughout the registration process (available in a range of languages).

(ii)

As stipulated in the **Company Law of the People's Republic of China 2018**, no legal corporations in mainland China are registered in English. Therefore, when searching the company registrar, individuals must enter the **company's name in Chinese** or enter the **18 digital Unified Social Credit Code.**

(iii)

Commentary

Access to Public Information

https://www.stats.gov.cn/english/ (i)

https://www.cecc.gov/publications/commission-analysis/china-commits-to-open-government-information-effective-may-1-2008#:~:text=In%20a%20move%20that%20Chinese,Information%20(OGI%20Regulation)%2C%20which (ii)

The **National Bureau of Statistics of China (NBS)** – information request form can be completed via the NBS website.

(i)

In 2008, the Chinese Government committed to **the Open Government Information Regulation (OGI Regulation)**. The purpose of this regulation was to combat corruption, increase public transparency and ensure citizens have access to public-held information.

The main features of the OGI are as follows:

1. All government agencies are **obliged to disclose** certain information, usually within **20 business days**
2. Citizens, legal persons and other organizations may **request information** and are entitled to receive a reply within 15 business days and **no later than 30 business days**

(ii)

Other

https://english.www.gov.cn/ (i)

https://www.gov.cn/home/2023-03/29/content_5748953.htm (ii)

The Chinese central government's Official web portal.

(i)

The State Council department website – includes links to the websites of the Ministry of Foreign Affairs, the Ministry of National Defence, etc.

(ii)

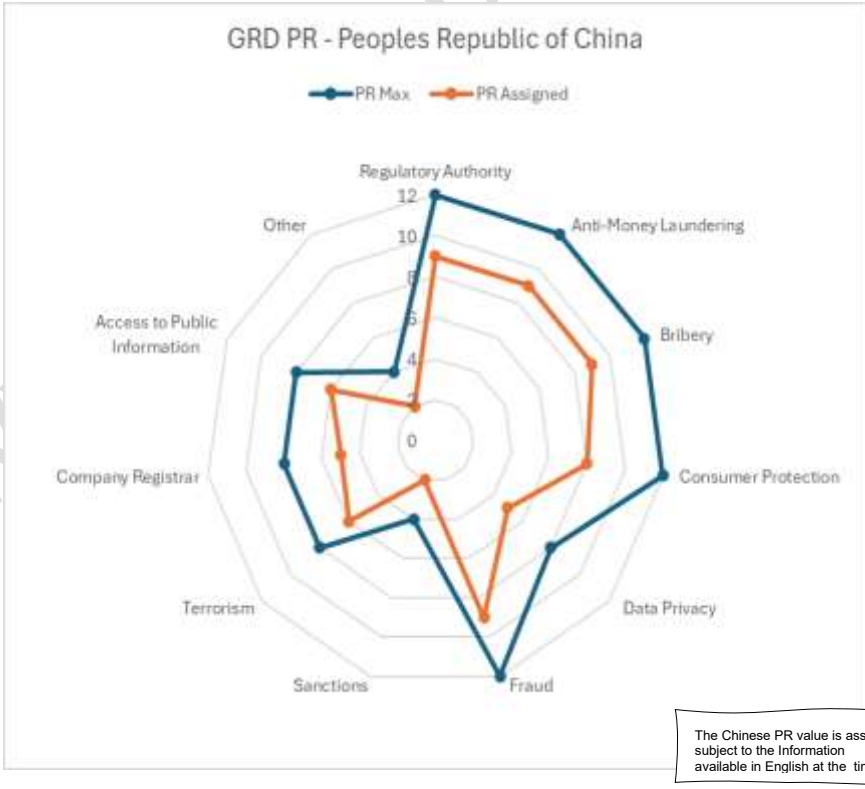
Posture Rating – China

The PR value of **7.0** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	9	9	9	8	5	9	2	6	5	6	2

China has a set of well-defined processes, regulations and laws allowing for compliance of the domains. However, the assigned value reflects the dominance of Mandarin on its digital channels and the absence of a central data protection authority.

NB: The figure does not reflect the execution of any processes, laws or regulations



The Chinese PR value is assigned subject to the Information available in English at the time of

.

Peoples Republic of China - Hong Kong

Commentary

Financial Regulatory Authority

https://www.hkma.gov.hk/eng/ (i)
https://www.sfc.hk/en/ (ii)

The Hong Kong Monetary Authority (**HKMA**) is the government authority in Hong Kong responsible for maintaining monetary and banking stability.

The HKMA is an integral part of the Hong Kong Special Administrative Region Government but operates with a high degree of autonomy, complemented by a high degree of accountability and transparency.

HKMA has four main pillars in relation to its functions:

1. Maintaining currency stability within the framework of the Linked Exchange Rate System
2. Promoting the stability and integrity of the financial system, including the banking system
3. Helping to maintain Hong Kong's status as an international financial centre, including the maintenance and development of Hong Kong's financial infrastructure; and
4. Managing the Exchange Fund

(i)

The Securities and Futures Commission (**SFC**) is an independent statutory body set up in 1989 to regulate Hong Kong's securities and futures markets and issues codes and guidelines to help industry participants comply with the laws.

(ii)

The Hong Kong **dollar** is the official currency of Hong Kong.

AI Act / Policy

https://gia.info.gov.hk/general/202410/28/P2024102800154_475819_1_1730083937115.pdf (i)
https://www.news.gov.hk/eng/2025/02/20250226/20250226_093511_297.html (ii)

In 2024, the Financial Services and the Treasury Bureau (**FSTB**) issued a policy statement on the responsible application of artificial intelligence in the financial market, outlining the Government's policy stance and how it intends to address some of the key challenges.

(i)

In 2025, the Financial Secretary of Hong Kong announced that the Government would be investing $1b. This, alongside the launch of HKGAI V1 shows the country's strong commitment to AI.

(ii)

HKGAI V1 is a large language model (LLM), its first locally developed generative artificial intelligence. HKGAI V1 was developed by the Hong Kong Generative AI Research and Development Center, a government-backed joint-university collaborative venture led by the Hong Kong University of Science and Technology (**HKUST**).

https://www.sfc.hk/en/Rules-and-standards/Anti-money-laundering-and-counter-financing-of-terrorism (i)

URL https://www.elegislation.gov.hk/hk/cap615!en (ii)

https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/infrastructure/svf/Guideline_on_AMLCFT_for_SVF_eng_Sep2020.pdf (iii)

https://www.fatf-gafi.org/en/countries/detail/Hong-Kong-China.html (iv)

The **Securities and Futures Commission** of Hong Kong and presents a list of relevant legislation and ordinances related to anti-money laundering and the countering of the financing of terrorist activities. (i)

As outlined by the Securities Commission, one of the primary pieces of legislation governing money laundering in Hong Kong is the Anti-Money Laundering and Counter Terrorist Financing Ordinance (**AMLO**). Some of the main features of the Ordinance include:

1. Imposing customer due diligence and record-keeping requirements on specified financial institutions
2. Combatting anti-money laundering (AML), potentially extending to virtual assets
3. Encompassing a broad scope of AML policy
4. Monitoring designated entities and activities, possibly including precious stones and metals
5. Regulating money service operations and the licensing of trust/company service providers
6. Establishing penalties for AML and other financial crimes

The Securities Commission outlines other relevant links to the bodies in force to counter money laundering. This list is not exhaustive, but refers to the following:

1. The Drug Trafficking (Recovery of Proceeds) Ordinance – **DTROP**
2. Organised and Serious Crimes Ordinance – **OSCO**
3. The United Nations Anti-Terrorism Measures Ordinance – **UNATMO**
4. The United Nations Sanctions Ordinance – **UNSO**
5. The weapons of mass destruction (control of provision of Services) Ordinance – **WMD CPS** (ii)

The Hong Kong Monetary Authority (**HKMA**) has also published a list of guidelines relating to Anti-Money Laundering and the Countering of Terror Financing for Stored Value Facility (**SVF**) Licensees. This encapsulates the approach taken by Hong Kong and its constituent bodies to curb the issue of money laundering and includes information relating to customer due diligence, record-keeping and wire-transfers. Hong Kong's Anti-Money Laundering regime is expansive and demonstrates a focussed commitment on the need to tackle the issues which may be pervasive in both a domestic and an international context **Chapter 3, section 9 (3.9)** of the guidelines is particularly important as it focusses on the duties and inherent obligations of the compliance officer and the Money Laundering Reporting Officer with relation to their role relating to a SVF.

A SVF is a payment system which allows customers to store funds for future payments.

(iii)

Hong Kong has been a member of **FATF** (Financial Action Task Force) since 1991. In 2019, it was assessed by two the **APG** (Asia-Pacific Group) and the FATF in terms of its ability to tackle money laundering and terrorist financing, with the recommendations being taken to adapt and improve its framework. Through its mutual evaluation report there was a thorough and in-depth review of Hong Kong's capacity to combat issues which related to these two areas. Currently Hong Kong is compliant on 11 recommendations and largely compliant on 25. Examples of areas in which it was deemed to be compliant include in

Financial Institution Secrecy Laws (R.9) and Targeted Financial Sanctions Related to Terrorism and Terrorist Financing (R.6). (iv)

Bribery

https://www.elegislation.gov.hk/hk/cap201!en (i)
https://www.icac.org.hk/en/about/power/index.html (ii)

The **Prevention of Bribery Ordinance (Cap. 201), or PBO,** is a comprehensive piece of anti-corruption legislation in Hong Kong, covering a broad spectrum of bribery offences in both the private and public sector. Some of the Law's main features include:

1. Provisions for preventing bribery in the **public sector** i.e. bribery concerning public servants, government contracts and auctions
2. Provisions for preventing bribery in the **private sector** i.e. involving principals of private businesses, companies or organizations
3. Powers of the relevant enforcement agency – the **Independent Commission Against Corruption (ICAC)** (i)

The ICAC implement a range of measures to combat bribery, as specified in the PBO. These include:

1. **Identifying transactions/ concealed assets** e.g. through searching bank accounts, holding and examining business and private documents and requesting suspects to provide details of their assets
2. **Detaining travel documents** of subjects and restraining the disposal of property to prevent offenders from fleeing Hong Kong
3. **Protecting confidentiality** of investigations (ii)

Consumer Protection

https://www.consumer.org.hk/en

The Hong Kong Consumer Council (*the "Council"*) is a statutory body for consumer protection in Hong Kong and is mandated to study and promote the protection of consumer rights. The Chairman, Vice-Chairman and members are all appointed by the Government of the HKSAR for a term not exceeding 2 years.

The Council Decree prescribes the following functions for the Council:

1. Collecting, receiving and disseminating information concerning goods and services and fixed property
2. Receiving and assessing complaints and providing advice to consumers of goods and services and purchasers, mortgagors and lessees of property
3. Taking such action as it thinks justified by information in its possession, including tendering advice to the Government or to any public officer
4. Encouraging businesses and professional associations to establish codes of practice to regulate the activities of their members

Commentary

Cloud Policy

https://www.govcert.gov.hk/doc/PG%20for%20Cloud%20Computing%20Security_EN.pdf (i)

https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2022/20220831e1.pdf (ii)

The Digital Policy Office Practice Guide for Cloud Computing Security.

(i)

The Hong Kong Monetary Authority Guidance on Cloud Computing.

(ii)

Data / Privacy

https://www.pcpd.org.hk/ (i)

https://www.pcpd.org.hk/english/complaints/doxxing/files/b202107161_Eng.pdf (ii)

The official website of the Office of the Privacy Commissioner for Personal Data (**PCPD**) the independent body set up to oversee the implementation of and compliance with the provisions of the Personal Data (Privacy) Ordinance (Chapter 486 of the Laws of Hong Kong) (PDPO).

The Personal Data (Privacy) Ordinance (the "**PDPO**") is applicable to both the private and the public sectors.

(i)

The Personal Data (Privacy) (Amendment) Bill 2021 (Bill gazetted on 16 July 2021) amends original PDPO, primarily focussing on:

1. Adapting and creating new offences for disclosing personal data without consent
2. Empowering the Privacy Commissioner for Personal Data with additional investigative and enforcement powers

(ii)

Fraud

https://www.elegislation.gov.hk/hk/cap210?xpid=ID_1438402833316_003

On the HK Government Website e-legislation portal, accessed by the above link, users can find relevant information relating to the statutes and laws in place to govern and penalise offences such as fraud (section 16A) which is found under the short title - ***'Theft Ordinance'*** on the portal. According to **Section 16A**.1, fraud is defined by the intent to deceive or defraud, where this action results in a benefit to someone else. **Section 17** also covers the offense of obtaining property by means of deception.

Sanctions

https://www.hkma.gov.hk/eng/key-functions/banking/anti-money-laundering-and-counter-financing-of-terrorism/sanctions-related-notices-updates/

UN sanctions are generally implemented in Hong Kong through regulations under the **United Nations Sanctions Decree.**

Hong Kong does not implement sanctions above and beyond those imposed by the United Nations Security Council ("**UNSC**").

Terrorism

https://www.sb.gov.hk/eng/special/terrorist/terrorist.html (i)
https://www.gld.gov.hk/egazette/english/gazette/file.php?year=2025&vol=29&no=7&extra=1&type=0&number=7 (ii)
https://www.police.gov.hk/ppp_en/04_crime_matters/cti/idctu.html (iii)

Hong Kong is a member of the UN and is thus duty-bound to adhere to its regulations through the inherent benefit conferred by membership. As such, on the Security Bureau's website, there are up-to-date lists relating to the United Nations (**Anti-Terrorism Measures (Cap.575)**), including the specifications of names and persons designated as terrorists or terrorist associates by Committees of the United Nations Security Council, catalogued by Government Notice Number.

(i)

The most recent example can be found through the corresponding URL.

(ii)

On a domestic level, more information can be gleaned regarding the attempts to confront terrorism and the financing of terror and terror-related activities. On the Hong Kong Police Force's website, there is a reference made to the Inter-Departmental Counter Terrorism Unit (**ICTU**), set up in April 2018. This Unit is comprised of multiple different entities and enforcement agencies, including the Hong Kong Police Force, the Immigration Department, the Customs and Excise Department, the Correction Service Department, the Fire Services Department and the Government Flying Service. This joint effort between policing and enforcement authorities aims to counter terrorism by establishing a platform for coordinated action and collaborative efforts within a group setting to tackle terrorism nationwide. The fundamental aspect central to the Unit's strength is the intelligence sharing mechanisms in place and the inter-departmental flow of information, which ensures a more robust CT initiative. There are also enhanced training measures in place and personnel support to aid in this venture.

(iii)

The **Law Society of Hong Kong** is responsible for overseeing law firms' compliance with Hong Kong's AML/CFT framework. To fulfil this responsibility, the Law Society conducted a sector-wide **AML/CFT risk assessment in 2022**. The purpose of this assessment, detailed in the following link, was to:

1. **Confirm** the Law Society's capacity for oversight in the Hong Kong Legal Sector
2. **Reduce** AML/CFT vulnerabilities and weaknesses
3. **Monitor** and report on emerging risks in this space
4. **Apply** AML/CFT/CPF supervision and protocol reviews

The risk assessment focused on five key areas: client risk, geographical risk, products and services, delivery channels and types of transactions.

(iv)

Commentary

Company Registrar

https://www.cr.gov.hk/en/home/index.htm (i)
https://www.cr.gov.hk/en/electronic/e-servicesportal/e-search.htm (ii)
https://www.e-services.cr.gov.hk/ICRIS3EP/system/dashboard/e-search.do (iii)

The Companies Registry website outlines step-by-step guidelines on **how to register** a new company in Hong Kong. This includes:

1. Guidelines on choosing the company's type and name
2. Information on how to deliver the application and relevant forms to be filled out
3. Process of collecting certificates

(i)

Registered companies in Hong Kong can be **searched** via the e-services portal.

(ii)

Unregistered users must use a different page than registered users and are required to input more detailed searcher information.

(iii)

Access to Public Information

https://www.access.gov.hk/en/home/index.htm I (i)
https://www.access.gov.hk/en/howtomakeinfo/index.html (ii)

The **Code on Access to Information** provides a formal framework for accessing information held by government bodies.

(i)

Hong Kong's Government website has a link to the required application form for requesting information held by government departments. The website also lists the Access to Information Officer's contact details for each government department.

(ii)

Other

https://www.gov.hk/en/residents/ (i)
https://www.gov.hk/en/about/govdirectory/govwebsite/#p3 (ii)
https://brdr.hkma.gov.hk/eng/doc-ldg/docId/getPdf/20250411-1-EN/20250411-1-EN.pdf (iii)

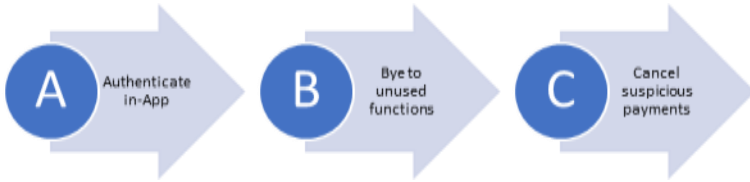
The gov.hk website is a one-stop portal of the Hong Kong Special Administrative Region Government.

(i)

Government and related organizations listed by organizational structure.

(ii)

Recent announcement (1 April 2025) from the Hong Kong Monetary Authority (**HKMA**) regarding new anti-digital fraud measures: “E-Banking Security ABC” where;



(iii)

Posture Rating - Hong Kong

The PR value of **7.2** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	9	9	9	7	6	8	2	6	7	7	2

While Hong Kong scores well in all domains, there's a notable lack of citizen interaction channels in the consumer and fraud sectors. Nevertheless, we found the available channels to be well-structured, a strength acknowledged in the assigned value.

NB: **The figure does not reflect the execution of any processes, laws or regulations.**

Qatar

Commentary

Financial Regulatory Authority

https://www.qcb.gov.qa/en/Pages/default.aspx (i)
https://www.qfcra.com/ (ii)
https://www.qfma.org.qa/English/pages/default.aspx (iii)

The **Qatar Central Bank** is the central bank of Qatar. Originally known as the Qatar Monetary Agency it was founded in 1973.

The main objectives and principles of the QCB are defined by the Law of the Qatar Central Bank and the Regulation of financial Institutions Issued by virtue of **Law no. 13, 2012**. These include:

1. Preserving currency value and assuring monetary stability.
2. Acting as a regulatory body for all financial services, businesses, markets and activities inside or through the state of Qatar, ensuring compliance with best international standards and practises.
3. Promoting financial and price stability.

(i)

Qatar Financial Centre (**QFC**) Regulatory Authority is the independent regulator of the QFC and was established to authorise and regulate firms and individuals conducting financial services in or from the QFC. It was established by **Law No. 7 of 2005** of the State of Qatar.

(ii)

Qatar Financial Markets Authority (**QFMA**) was established under the **Law No. 33 of 2005** regarding the establishment of Qatar Financial Markets Authority to regulate and supervise the financial markets in Qatar.

(iii)

The national currency of Qatar is the Qatari **riyal**.

AI Act / Policy

https://assurance.ncsa.gov.qa/en/publications/policy (i)
https://www.mcit.gov.qa/wp-content/uploads/sites/4/2024/09/digital_agenda_2030_full_version_english.pdf?csrt=11183559697057584732 (ii)

Qatar does not currently have any legally binding laws in relation to AI. However, the **National Security Agency, 2024**, released a document outlining guidelines for organizations on how to securely use/adopt AI and forms part of the Digital Agenda 20230 (**DA2030**).

(i)

The goal of DA2030 is to establish Qatar as a leading digital economy powered by an *attractive and efficient business environment with high-yield digital investments*". Through **Hyper Automation** Qatar seeks to increase the amount of compute used in the largest AI training runs and thus position itself as a leader in the field.

(ii)

Commentary

Anti-Money Laundering

https://www.moci.gov.qa/en/anti-money-laundering-and-terrorism-financing/

The **Anti-Money Laundering and Terrorism Financing (AML/CFT)** section was introduced under the Companies Affairs Department at MOCI, in accordance with the **Decision No. (95) of 2019.** Some of the key elements of the section with relevance to anti-money laundering are as follows:

1. Coordinated efforts with the **National Anti-Money Laundering and Terrorism Financing Committee (NAMLC)**, providing relevant information and data and collaborating on National Risk Assessments.
2. Sectoral risk assessments of legal entities and designated non-financial businesses and professions who are registered with and supervised by the **Ministry of Commerce and Industry**.

Bribery

https://www.almeezan.qa/LawArticles.aspx?LawTreeSectionID=201&lawId=26&language=en

In accordance with **Law No. 11 of 2004 Issuing the Penal Code**, bribery is defined by any public officer who asks for or accepts, for themselves or another party, money, benefit or a simple promise for something in exchange for carrying out (or abstaining from carrying out) an activity under the remits of their office.

The same principles also apply in a professional setting; any employee who asks for money or a benefit without the knowledge of their employer in exchange for undertaking duties assigned to them (or abstaining carrying out those duties) will be held liable for accepting bribery.

The URL directs users to the Qatari Legal Portal.

Consumer Protection

https://www.almeezan.qa/LawPage.aspx?id=2647&language=en (i)
https://www.almeezan.qa/LawArticles.aspx?LawTreeSectionID=9818&lawId=2647&language=en (ii)

Qatar's **Law No. 8 of 2008 on Consumer Protection** is comprised of various elements, including: consumer rights, supplier obligations, sanctions and general provisions.

(i)

According to **Article 2** of this law, no person will be permitted to conduct any activity if it is in breach of basic consumer rights. Some of the rights stipulated in this law are as follows (*the full list can be found on the Ministry of Justice website*):

1. The right to obtain correct data and information about commodities and services
2. The right to choose commodities that meet conditions of quality and conform to specifications
3. The right to safety and protection from commodities or services that are unsafe

(ii)

Under **Article 4** and in accordance with **Law No. 12 of 2004**, private associations and foundations whose activities relate to consumer protection may be established under specified conditions (*these can be found on the Ministry of Justice website ii*).

Commentary

Cloud Policy

https://www.cra.gov.qa/en/document/cloud-policy-framework

available to download as PDF in English/Arabic (ii)

https://www.cra.gov.qa/document/regulation-for-cloud-data-interoperability-and-data-portability (i)

The Communications Regulatory Authority released the **Cloud Policy Framework** in 2022. This document outlines policy and regulatory recommendations for cloud computing within Qatar, calling for high levels of cooperation between government entities and private stakeholders to promote the development of a robust cloud industry in Qatar.

(i)

The **Regulation for Cloud Data Interoperability and Data Portability**, issued by the Communications Regulatory Authority (**CRA**), provides recommendations regarding data interoperability and data portability for the above Cloud Policy Framework.

(ii)

Data / Privacy

https://assurance.ncsa.gov.qa/en/privacy/law (i)

https://www.almeezan.qa/ (ii)

In 2016, the then Emir of the State of Qatar, HH Sheikh Tamim Bin Hamad Al-Thani issued **Law No.13 on Personal Data Privacy and Protection**.

The law is enforced by the National Cyber Governance and Assurance Affairs department, who supervise the processing of personal data within the state of Qatar.

The main features of the new law include:

1. Increased stringency in procedures employed by businesses when processing personal data (not applying to personal data processed by individuals privately)
2. Introduction of requirements for organizational training and proactively implementing policies to safeguard personal data from loss, damage, modification, disclosure or unauthorised access
3. Restriction of how organizations process personal information/perform marketing activities, with explicit consent required before undertaking any activities
4. Obligation of organizations to outline scope of data processing and obtain consent from parent/legal guardian in the instance that their services are used by minors

(i)

The full details of the law can be found on the Qatari legal portal.

(ii)

Commentary

Fraud

https://www.almeezan.qa/LawArticles.aspx?LawTreeSectionID=8907&lawId=2559&language=en (i)
https://www.qfcra.com/financial-scams/ (ii)
https://www.moci.gov.qa/en/about-the-ministry/departments/departments-under-the-assistant-deputy-of-consumer-affairs/the-consumer-protection-and-combating-commercial-fraud/ (iii)

In accordance with **Law no (22) of 2004 Regarding Promulgating the Civil Code**, a contract may be declared void if it can be proven that it was accepted because of deception i.e., fraud. Furthermore, if it can be proven that an individual lied or intentionally withheld facts pertaining to the contract, they will also be liable for fraud. (i)

The **Qatar Financial Centre (QFC) Regulatory Authority** regulates against scams linked to financial services activities carried out by authorised firms (or those claiming to be), e.g., investment scams, insurance policy scams, financial services scams. (ii)

The Consumer Protection and Combatting Commercial Fraud Department which sits under the **Ministry of Commerce and Industry** are responsible for governing commercial fraud. This includes implementing legislation to combat commercial fraud, reviewing and responding to commercial fraud complaints and preventing fraud by collaborating with retailers and authorities. (iii)

Sanctions

https://www.moci.gov.qa/en/anti-money-laundering-and-terrorism-financing/legal-framework/sanctions-list/

A unified record of persons and entities on Qatar's sanction list can be accessed via the Ministry of Interior – National Counter Terrorism Committee website.

The website also provides a free online search tool.

Terrorism

https://www.moci.gov.qa/wp-content/uploads/2021/08/Law-No.-27-of-2019-Promulgating-the-Law-on-Combatting-Terrorism-1.pdf

Qatar's strategy on combatting terrorism is enshrined in **Law No. (27) of 2019**, **Promulgating the Law on Combatting Terrorism**.

The law stipulates that the relevant supervisory authorities have the right to "*supervise, follow-up, monitor and ensure compliance*" by financial institutions with the implementation of targeted financial sanctions against terrorism and terrorist financing.

Company Registrar

https://www.moci.gov.qa/en/our-services/investor/companies-type/ (i)
https://eservices.qfc.qa/qfcpublicregister/publicregister.aspx (ii)

The Ministry of Commerce and Industry – **MOCI** is responsible for the regulation of trade and industrial activities in Qatar. (i)

The Qatar Financial Centre maintains a capability to search registered companies. (ii)

Access to Public

https://www.acta.gov.qa/en-us/ProjectsAndAchievements/Pages/transparency-in-access-to-information.aspx

The Administrative of Control and Transparency Authority (**ACTA**) prevents and combats corruption, considering the standards and requirements set out **Amiri Decree no. (6) of 2015**.

Other

https://www.gco.gov.qa/en/

The official website of the Government Communications Office.

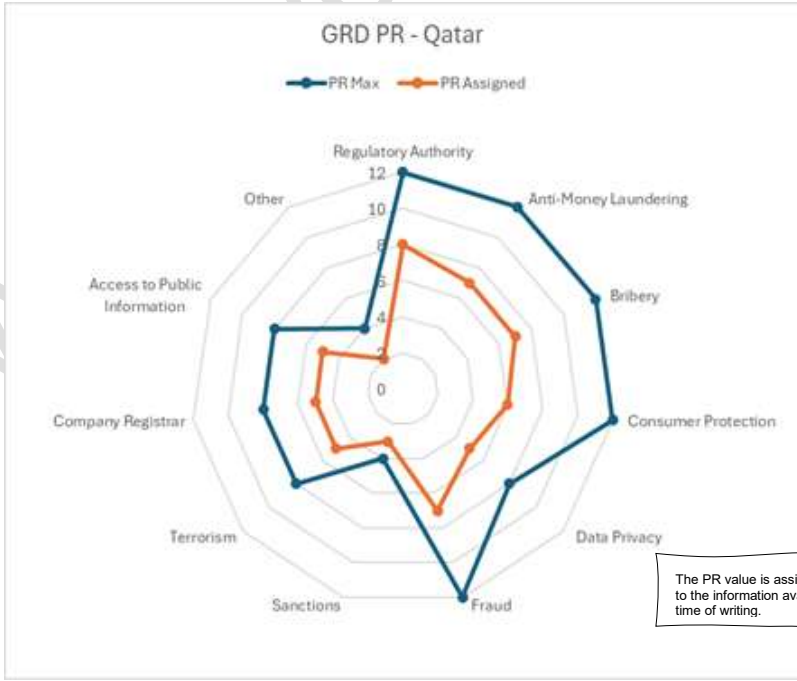
Posture Rating - Qatar

The PR value of **6.0** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	8	7	7	6	5	7	3	5	5	5	2

Qatar has established numerous laws and supporting government bodies. However, its digital services are currently fragmented. This is set to change with the implementation of the Digital Agenda 2030, which emphasizes integrated digital channels and as such, has been reflected in the assigned PR value.

NB: **The figure does not reflect the execution of any processes, laws or regulations**.



Republic of South Africa

Commentary

https://www.resbank.co.za/en/home (i)

https://www.fsca.co.za/Pages/Default.aspx (ii)

The South African Reserve Bank (**SARB**) is the central bank of South Africa with the primary objective to protect the value of the currency and has the responsibilities depicted below:

(i)

Figure 31 South African Reserve Bank Responsibilities

The Financial Sector Conduct Authority (**FSCA**) is the market conduct regulator in South Africa's Twin Peaks regulatory model implemented via the Financial Sector Regulation Act. The FSCA has four objectives:

1. **Protect** financial customers by promoting their fair treatment by financial institutions
2. Enhance and support the efficiency and **integrity** of financial markets;
3. Provide financial **education** and promote financial literacy
4. Assist in maintaining financial **stability**

(ii)

The South African **rand** is the official currency of South Africa.

Commentary

AI Act / Policy

https://www.dcdt.gov.za/sa-national-ai-policy-framework/file/338-sa-national-ai-policy-framework.html (i)

https://www.dcdt.gov.za/images/phocadownload/AI_Government_Summit/National_AI_Government_Summit_Discussion_Document.pdf (ii)

The **National Artificial Intelligence (AI) Policy Framework for South Africa 2024** aims to stimulate the integration of Artificial Intelligence technologies to drive economic growth, enhance societal well-being and position South Africa as a leader in AI innovation - South African National AI Policy Framework. (i)

South Africa's **Artificial Intelligence (AI) Planning: Adoption of AI by the Government** paper was issued by the Department of Communications and Digital Technologies (**DCDT**) in Oct 2023. The primary aim of this document was to develop a South African National AI Plan. This plan will serve as a foundation for establishing a clear legal and governance framework, as well as an AI regulatory landscape, informed by collaborative stakeholder input. Additionally, it will contribute to broader coordinated AI initiatives across the African continent. (ii)

https://www.fic.gov.za/wp-content/uploads/2023/10/Financial-Intelligence-Centre-Act-2001-Act-38-of-2001.pdf (i)

https://www.fic.gov.za/about/#what-the-fic-does (ii)

https://www.resbank.co.za/en/home/what-we-do/Prudentialregulation/anti-money-laundering-and-countering-the-financing-of-terrorism (iii)

https://www.fsca.co.za/Regulatory%20Frameworks/Pages/AMLCFT.aspx (iii)

The **Financial Intelligence Act of 2001 (amended in 2017)** is one of the central legislations governing money laundering in South Africa. Some of the key features of the Act include:

1. The establishment of the Financial Intelligence Centre (**FIC**) – South Africa's **financial intelligence unit**
2. **Obligations of supervised institutions,** i.e. customer due diligence, record keeping and reporting obligations
3. Implementation of measures according to resolutions adopted by the **Security Council of the United Nations**
4. **Powers of the FIC** to supervise and enforce compliance of entities under their supervision.

(i)

The FIC is mandated to identify the proceeds of crime, contributing to the fight against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. Some of their main functions include:

1. **Receives and analyzes** regulatory reports and disseminates information to relevant regulatory authorities
2. **Facilitates supervision** and enforcement by supervisory bodies
3. **Exchanges information** with bodies from other countries with similar ML,TF and PF objectives

(ii)

As stipulated in the FIC Act, the **Prudential Authority (PA) of the South African Reserve Bank** is responsible for AML/CFT supervision of banks, mutual banks and life insurers.

(iii)

The Financial Sector Conduct Authority (**FSCA**) is responsible for supervising and enforcing compliance with the **FIC Act** by authorized users of an exchange, collective investment scheme managers and financial services providers.

The FSCA has a dedicated **AML/CFT supervision department** (contact details available via their website). The department operates on a risk-based approach, with some of its main activities including:

1. **Offsite supervision,** e.g. issuing directives
2. **Onsite inspections** and thematic reviews
3. **Raising awareness** to increase compliance among supervised entities through webinars, surveys, etc.

(iii)

Bribery

https://www.gov.za/documents/prevention-and-combating-corrupt-activities-act-0 (i)
https://www.gov.za/sites/default/files/gcis_document/202105/national-anti-corruption-strategy-2020-2030.pdf (ii)
https://www.stateofthenation.gov.za/state-capture-commission-recommendations/type/permanent-anti-corruption-commission (iii)
https://www.gov.za/sites/default/files/anti_corruption_hotlines.pdf (iv)

South Africa's most significant law concerning combatting corruption and bribery is the **Prevention and Combating of Corrupt Activities Act 12 of 2004.** The Act defines bribery as a form of corruption, criminalising bribery in both the **public and private sectors.**

(i)

As specified in the **National Anti-Corruption Strategy 2020-2030,** the South African Government has adopted a multi-agency approach to combatting bribery and corruption. This involves the following authorities:

1. **Oversight and regulatory bodies** e.g. parliament committees such as the Standing Committee on Public Accounts (**SCOPA**)
2. **Existing agencies and specialised units/structures** e.g. the Department of Public Service and Administration, which plays a key role in setting norms and standards on ethics, integrity and anti-corruption in the public sector
3. **Coordinating bodies** such as the Clusters of Directors-General and Clusters of Ministers, working together to ensure an integrated approach to the implementation of government priorities and programmes

On an **international level**, South Africa has ratified various international conventions and treaties and participates in forums that require the country to implement measures to prevent and combat corrupt activities. This includes:

- The OECD's Anti-bribery Convention
- The United Nations Convention against Corruption (**UNCAC**)

(ii)

South Africa also established the **Anti-State Capture and Corruption Commission.** Their primary purpose is to **investigate and publicly expose** acts of state capture and corruption in the public sector, including state organs. Furthermore, they are responsible for ensuring Parliament effectively carries out its **oversight functions**, making **recommendations to the President** where required.

(iii)

A list of **national anti-corruption hotlines** is available via the Government website for individuals wishing to report a bribery or corruption offence.

(iv)

Commentary

Consumer Protection

https://thencc.org.za/what-we-do/ (i)

https://www.ncr.org.za/ (ii)

The National Consumer Commission is one of the key regulatory authorities concerned with governing consumer protection in South Africa. Guided by **Section 85 of the Consumer Protection Act (CPA),** some of their main functions include**:**

- Improving consumer protection by **educating the public and raising awareness**
- **Promoting higher levels of compliance** with the CPA through guided interventions with businesses
- **Receiving complaints** and processing them in accordance with the provisions of the CPA.

(i)

The National Credit Regulator (**NCR**) is mandated to promote a fair and non-discriminatory consumer-credit marketplace.

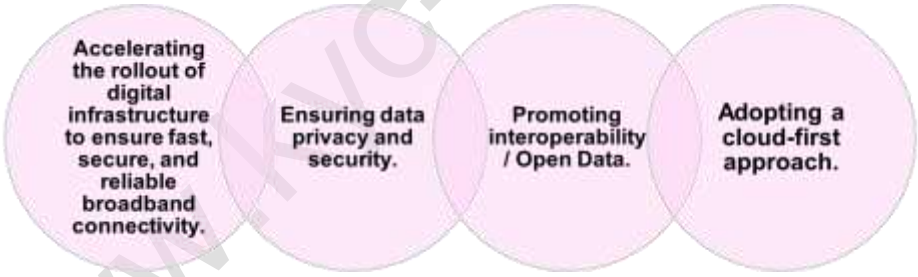
The NCR has a range of responsibilities, including credit granting, prohibiting reckless lending and protecting consumers through the enforcement of the National Credit Act, No. 34 of 2005 (**NCA**).

(ii)

Cloud Policy

https://www.gov.za/sites/default/files/gcis_document/202406/50741gen2533.pdf

The **South African National Policy on Data and Cloud** (March 2024) released by the Department of Communications and Digital Technologies, is framed on the following principles.



:

Figure 32 Key principles of the SA Cloud Policy

Data / Privacy

https://popia.co.za/

South Africa's data privacy is governed by the Protection of Personal Information Act, 2013 (**Act No. 4 of 2013**), otherwise known as the **POPIA**. The primary aim of the Act is to protect individuals' privacy and ensure the responsible processing of personal data.

The POPIA also addresses the transfer of personal information across international borders and sets out specific compliance standards for such transfers.

Commentary

Fraud

https://www.gov.za/sites/default/files/gcis_document/201409/a12-04.pdf (i)
https://www.gov.za/faq/justice-and-crime-prevention/how-do-i-report-fraud-or-corruption-state-department-or-state (ii)

The Prevention and Combating of Corrupt Activities Act No. 12 of 2004 (**PRECCA**) makes repeals or amendments to a range of laws in South Africa, many of which pertain to fraud. Some of the key changes include:

- **Expanding the situations** in which fraudulent activities are subject to criminal prosecution.
- **Increasing the responsibility** of businesses and institutions to prevent fraudulent and corrupt conduct.
- **Reinforcing the importance of reporting fraud**, introducing legal provisions to ensure relevant entities comply with reporting obligations.

(i)

Information on how to anonymously report an incident of fraud to South Africa's **anti-corruption hotline** is available via the Government website.

(ii)

Sanctions

https://www.fic.gov.za/targeted-financial-sanctions/ (i)
https://www.afdb.org/en/projects-operations/debarment-and-sanctions-procedures (ii)

South Africa's FIC hosts and maintains an updated list of proscribed persons and entities, as per the resolutions of the United Nations Security Council (**UNSC**).

The **Targeted Financial Sanctions (TFS) list** can be viewed via the FIC's online search tool.

N.B. South Africa does not implement its own domestic sanctions list; the TFS list solely represents the UNSC consolidated list of targeted financial sanctions.

(i)

South Africa is a signatory to the Agreement for Mutual Enforcement of Debarment Decisions. by the African Development Bank Group.

(ii)

Commentary

Terrorism

https://www.fic.gov.za/wp-content/uploads/2023/10/Financial-Intelligence-Centre-Act-2001-Act-38-of-2001.pdf (i)

https://nationalgovernment.co.za/units/view/42/state-security-agency-ssa (ii)

South Africa's FIC Act makes key provisions for combatting the financing of terrorism. This includes:

1. **Establishing the FIC**, responsible for detecting and preventing the flow of funds that could be used to support terrorism (amongst other duties).
2. **Mandating** the **Prudential Authority (PA) of the South African Reserve Bank** to supervise banks, mutual banks and life insurers regarding their AML/CFT activities.
3. **Facilitating** cooperation and information sharing with international partners.

(i)

The State Security Agency (**SSA**) also plays a central role in preventing and combatting terrorism in South Africa. Their mandate is to provide the government with intelligence on **domestic and foreign threats to national security**, enabling the government to implement policies that appropriately manage those threats.

(ii)

Company Registrar

https://eservices.cipc.co.za/ (i)

https://bizportal.gov.za/ (ii)

Companies in South Africa can be registered through the **Companies and Intellectual Property Commission**. Companies wishing to register must have a valid CIPC customer code.

Only **private and non-profit companies** can be registered with a standard memorandum of incorporation, all other company types must be filed manually.

(i)

The South African Company Registrar search function has been moved to the **BizPortal website**. Companies can be searched by enterprise number, name or ID number.

(ii)

Commentary

Access to Public Information

https://www.gov.za/sites/default/files/gcis_document/201409/a2-000.pdf (i)
https://www.gov.za/services/services-residents/information-government/access-information (ii)

The **Promotion of Access to Information, Act, 2000** ensures that citizens of South Africa can exercise their constitutional right of access to information held by the State or another person.

(i)

The Government website outlines clear guidelines for individuals wishing to request publicly held information:

1. Contact the **deputy information officer** of the relevant government department
2. Submit a Promotion of Access to Information (PAIA) form
3. If information is not already freely available, the individual must pay a **request fee** (and possibly an access and search fee if applicable)
4. Individuals are under **no obligation to state their reason** for requesting information

(ii)

PAIA forms can be requested directly from the office of the relevant department or, alternatively, downloaded from the **Information Regulator's website**.

The **Information Regulator** has the authority to oversee and ensure that both government agencies and private organizations adhere to the Promotion of Access to Information Act of 2000.

(iii)

Other

https://www.gov.za/ (i)
https://nationalgovernment.co.za/units/type/3/national-department (ii)

The official website of the Government of the Republic of South Africa.

(i)

The list of national government departments in South Africa and their subsequent clusters.

(ii)

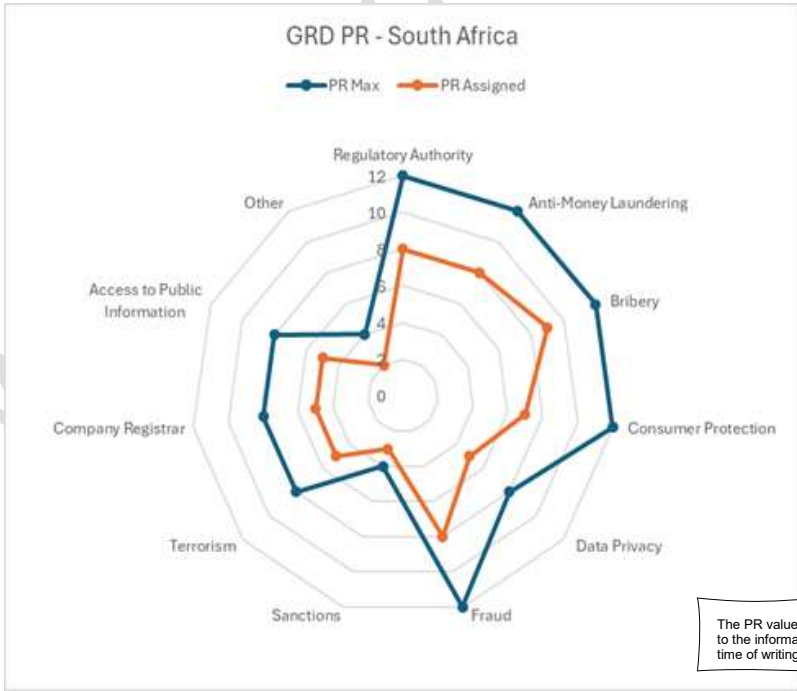
Posture Rating - South Africa

The PR value **6.5** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	8	8	9	7	5	8	3	5	5	5	2

South Africa is slowly maturing its processes, regulations and laws to meet its domain obligations. The provision of 'Hotlines' by the government channels is factored into the value assigned and reflects the available information at the time of writing.

NB: **The figure does not reflect the execution of any processes, laws or regulations.**



Russia (aka The Russian Federation)

Commentary

Financial Regulatory Authority

https://www.cbr.ru/eng/ (i)

http://archive.government.ru/eng/power/105/#:~:text=The%20Federal%20Service%20for%20Financial%20Markets%20(FSFR)%20is%20a%20federal,microfinance%2C%20commodity%20markets%2C%20exchange%20intermediaries (ii)

The Central Bank of the Russian Federation is Russia's central bank, also commonly referred to as the "**Bank of Russia**".

The Bank of Russia has numerous functions, its primary role being the issuance of currency and the protection and stability of the currency. A comprehensive list of the Bank's functions is provided below.

Figure 33 The many functions of the Bank of Russia

(i)

The Federal Service for Financial Markets (**FSFR**) is a federal executive body responsible for legal regulation, control and supervision of financial markets (excluding banking and auditing), including regulation and supervision of insurance, credit cooperation and microfinance, commodity markets, exchange intermediaries and brokers and the formation and investment of pension funds, including the payment reserve, as well as for government control over compliance with Russian laws to prevent insider trading and market manipulation.

(ii)

The Russian **rouble or Ruble** is the official currency of the Russian Federation.

Commentary

AI Act / Policy

https://a-ai.ru/?lang=en

At the time of writing, limited concrete information was available regarding advancements in AI within Russia. However, Russia's recent announcement of its intention to collaborate on AI development with BRICS partners, particularly China and other nations, suggests that future developments are likely.

Established in 2019, the AI Alliance serves as the primary driving force behind AI advancement in Russia.

Anti-Money Laundering

https://www.cbr.ru/eng/counteraction_m_ter/#a_161565file (i)
https://www.cbr.ru/Content/Document/File/161565/press_31052024_e.pdf

The Russian AML/CFT system is made up of federal executive bodies, the Bank of Russia, other government bodies and organizations, banks, non-bank financial institutions, as well as enterprises and designated non-financial businesses and professions (the full list of obliged entities under the AML/CFT legislation is set out in **Article 5 of Federal Law No. 115-FZ**). (ii)

In 2022 the Bank of Russia launched the *Know Your Customer Platform*, a system that provides information about the risk level of potential and existing clients' involvement in suspicious transactions.

(ii)

Bribery

https://epp.genproc.gov.ru/web/eng_gprf/combating-corruption/anti-corruption-legislation?item=62556253 (i)
https://epp.genproc.gov.ru/web/eng_gprf/combating-corruption (ii)
https://www.oecd.org/en/topics/sub-issues/fighting-foreign-bribery/russia-country-monitoring.html (iii)

Federal Law No. 273-FZ on Combatting Corruption is the primary piece of legislation governing bribery and corruption in Russia.

Specifically, **Article 1** of the Law clearly defines what constitutes a corrupt offence, i.e. the "abuse of power, the giving of a bribe, the receiving of a bribe, abuse of authority, commercial bribery or other unlawful use by an individual of his or her official position".

(i)

The **Prosecution Service** is the principal authority responsible for the enforcement and implementation of anti-corruption legislation in Russia. Some of their main functions include:

1. **Initiating and conducting criminal proceedings** against individuals accused of bribery and corruption
2. **Oversight and supervision** of government bodies and officials
3. **Enforcing federal laws** related to anti-corruption

(ii)

As a Party to the **OECD Anti-Bribery Convention**, Russia's implementation of anti-bribery and corruption measures is also subject to rigorous peer review and monitoring by the **OECD Working Group on Bribery.**

(iii)

Commentary

Consumer Protection

http://rospotrebnadzor.ru/en/

The Federal Service for the Oversight of Consumer Protection and Welfare (**Rospotrebnadzor**) is the federal executive body responsible for drafting and implementing government policy and regulations in the field of consumer rights protection and for carrying out federal state sanitary and epidemiological supervision, including on the railways, to protect public health and the environment and federal state supervision of consumer rights protection.

N.B. At the time of writing, we found restrictions on site access from the UK.

Cloud Policy

In 2017 Russia banned all the tools that may help users bypass internet surveillance, including VPNs, proxies and Tor.

Individuals in Russia may only use government approved VPN services that log their online activity.

Data / Privacy

http://www.kremlin.ru/acts/bank/24154

The **Federal Law on Personal Data (No. 152-FZ),** also known as the Data Protection Act (**DPA**), is the main law governing data privacy. It generally requires data operators to store and process the personal data of citizens and hosted within Russia, although exceptions exist.

Fraud

Within the Russian legal system, fraud is defined as the unlawful acquisition of property or rights thereto through deceptive practices or the abuse of trust. Cybercrime is addressed in **Chapter 28 of the Criminal Code**, with specific articles pertaining to fraudulent activities involving electronic payments.

As of July 2024, credit institutions in Russia are obligated to **suspend monetary transfers for a period of two days** if the beneficiary's details are found in the Bank of Russia's database of actual and attempted fraudulent transactions. Non-compliance with this requirement obligates the institution to reimburse the client for the transferred funds within 30 calendar days.

Sanctions

https://www.fedsfm.ru/documents/terrorists-catalog-portal-act

Russia adheres to UN sanctions, citing the incorporation of universally recognized principles and rules of international law and its international treaties into its legal system. Typically, sanctions are implemented through Government Decrees based on Presidential Orders and relevant Federal Laws.

Terrorism

Russia's Federal Financial Monitoring Service (**Rosfinmonitoring**) is responsible for several key areas: combating money laundering and terrorist financing; creating and enacting state policies and legal frameworks in these domains; coordinating related work across federal executive bodies; and acting as the national center for threat assessment related to money laundering, terrorism financing and weapons proliferation, ultimately developing strategies to counter these risks. The Federal Financial Monitoring Service reports directly to the President of the Russian Federation.

The Federal Financial Monitoring Service reports directly to the President of the Russian Federation.

N.B. The URL is the full list of terrorists and extremists at the time of writing.

Commentary

Company Registrar

https://service.nalog.ru/gosreg/#ul (ii)
https://egrul.nalog.ru/index.html (i)

Information on how to register a company online in Russia is available via the **Federal Tax Service of Russia's website.** This includes registration of sole proprietors and legal entities.

(i)

The **Unified State Register of Individual Entrepreneurs** contains comprehensive information about companies registered in the Russian Federation. Individuals can search the register using either a Taxpayer Identification Number (**INN**) or Primary State Registration Number (**OGRN**).

(ii)

Access to Public Information

https://www.prlib.ru/en/node/433073

Russia's **Law on Providing Access to Information on the Activities of State Bodies and Local Authorities** establishes the right of Russian citizens to request and receive information from state and local government bodies.

The Law also outlines clear procedures for making requests, which can either be made in person, by post, or online.

Other

http://government.ru/en/ (i)
http://kremlin.ru/ (ii)
http://government.ru/en/gos_services/ (iii)

The official website for the Russian Government.

(i)

The official website for the President of Russia.

(ii)

The **Unified Portal of Public and Municipal Services** aims to facilitate interactions between citizens and the government and to make it easier to use government services.

(iii)

Posture Rating - Russia

The PR value of **6.5** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	9	9	8	6	5	8	2	5	5	5	3

Seemingly, Russia appears to have a highly bureaucratic system of processes to support its regulations and laws, most clearly illustrated by its Regulatory Authority Structure for meeting domain obligations.

We have segmented the score for “Sanctions” and “Terrorism” as the two are very closely related and proportioned the score as an indicator.

At the time of writing, we found limited information available on Government websites and resources, many of which placed restrictions on Internet traffic from our locations, which is reflected in the value assigned.

NB: The figure does not reflect the execution of any processes, laws or regulations.

Kingdom of Saudi Arabia

Commentary

Financial Regulatory Authority

https://sama.gov.sa/en-US/Pages/default.aspx (i)

https://cma.org.sa/ (ii)

The Saudi Central Bank (SAMA) , previously known as the Saudi Arabian Monetary Authority (**SAMA**) is the central bank of the Kingdom of Saudi Arabia. After a name change in 2020, the Saudi Central Bank continued to use the acronym SAMA to identify itself.

(i)

The functions performed by SAMA are shown below:

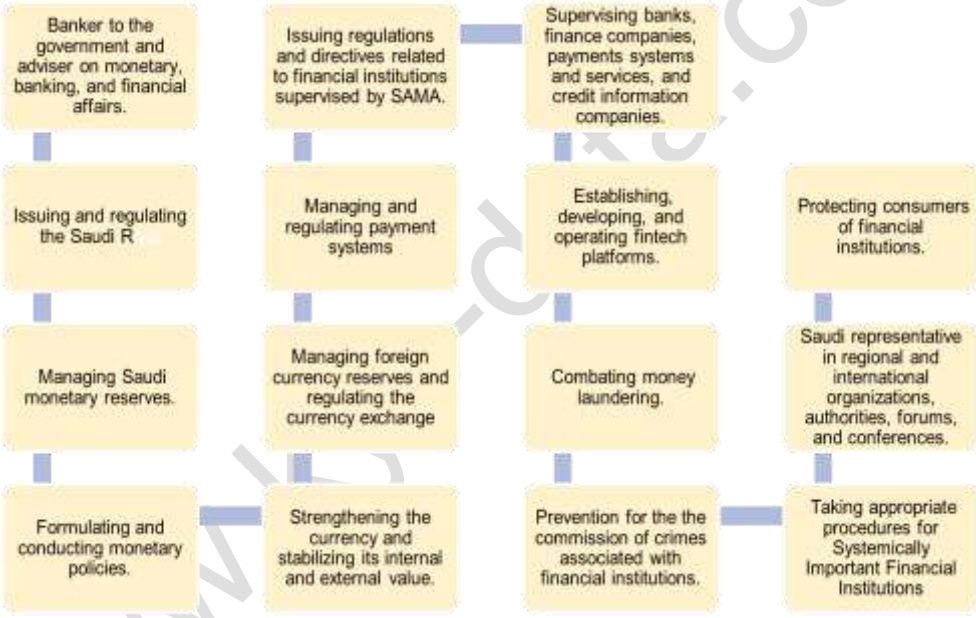


Figure 34 Core Functions of the Saudi Central Bank (SAMA)

The Capital Market Authority (**CMA**) is a government body that regulates and develops the Saudi Arabian Capital Market by issuing required rules and regulations for implementing the provisions of **Capital Market Law (No. (M/30) dated 2/6/1424H).**

The basic objective of the CMA is to create the investment environment, boost confidence and reinforce transparency and disclosure standards in all listed companies while protecting both investors and dealers from illegal acts in the market.

(ii)

The Saudi **riyal** is the currency of Saudi Arabia.

Commentary

AI Act / Policy

https://sdaia.gov.sa/en/SDAIA/Pages/default.aspx (i)

https://www.vision2030.gov.sa/en (ii)

The Saudi Data & AI Authority (**SDAIA**) is the competent authority in the Kingdom concerned with data and AI, including big data. The Authority has three main objectives:

1. Establishing the governance of data & AI
2. Promoting and ensuring the position of the Kingdom as a global leader in data-driven economies
3. Providing foresight and data-related capabilities and enhancing them through continuous innovation in the field of AI (i)

The Saudi **Vision 2030** is a blueprint for major digital transformation, aiming to diversify the economy, empower citizens, create a vibrant environment for both local and international investors and establish Saudi Arabia as a global leader in AI. (ii)

Anti-Money Laundering

https://www.aml.gov.sa/en-us/RulesAndRegulations/Anti-Money%20Laundering%20Law.pdf - **draft version** (i)

https://www.aml.gov.sa/en-us/Pages/About.aspx (ii)

The primary law governing money laundering in Saudi Arabia is the Anti-Money Laundering Law, 2017 (**AML Law**).

The AML Law covers a range of areas, including:

1. **Outlining** the various types of money laundering offences
2. **Preventative measures** e.g. duties of Financial Institutions (**FIs**), Designated Non-Financial Businesses and Professions (**DNFBPs**) to identify, assess and document money laundering risks and provide risk assessment reports to the supervisory authorities upon request
3. **Powers and duties of the General Directorate of Financial Intelligence** i.e. receiving and analysing suspicious transaction reports and disseminating analysis to competent authorities
4. **International cooperation** and the right of competent authorities to exchange information with foreign counterparts, in line with applicable statutory procedures

(i)

The Saudi Central Bank (**SAMA**) plays a central role in combatting money laundering in Saudi Arabia, establishing national preventative measures and procedures.

The Anti-Money Laundering Permanent Committee (**AMLPC**) was established primarily to implement the FATF's Forty Recommendations on combatting money laundering.

The AMLPC consists of members representing a **range of different regulatory bodies** in Saudi Arabia, including:

- The SAMA
- The Presidency of State Security
- Public Prosecution
- The Capital Market Authority

Since its formation in 1999, the Committee has been working to "enhance, streamline and develop the legal and institutional framework and related activities", ensuring it is in line with international standards. (ii)

Commentary

Bribery

https://laws.boe.gov.sa/Files/Download/?attId=0f617e25-0191-40e1-bf4b-adbb010ed141 (i)
https://www.nazaha.gov.sa/Index (ii)
https://www.nazaha.gov.sa/Services (iii)

The most consequential law concerning bribery in Saudi Arabia is the **Anti-Bribery Law Royal Decree No. M/36, 1992.** The scope of this law covers:

- Bribery of public officials
- Bribery in the private sector i.e. involving cooperative societies, private organizations, companies, sole proprietorships, or professional bodies
- Bribery of foreign public servants

(i)

The Oversight and Anti-Corruption Authority (**Nazaha**) is the primary regulatory body responsible for combatting bribery and corruption in Saudi Arabia. All bribery and corruption offences occurring within Saudi Arabia should be **reported directly to Nazaha**. This can be done by phone, email or in person.

(ii)

Beneficiaries may also **submit a report** to the Authority via Nazaha's website, outlining any details about actions involving corruption crimes, financial or administrative violations, or failure to provide public services to citizens.

(iii)

Consumer Protection

https://mc.gov.sa/en/About/Departments/cp/Pages/default.aspx (i)
https://mc.gov.sa/en/guides/Documents/CustomerGuide.pdf (ii)

The **Deputy Ministry of Consumer Protection** is the primary government agency concerned with consumer protection in Saudi Arabia. The Ministry performs a range of functions, including:

1. combatting commercial fraud in all its forms;
2. regulating commercial discounts and contests;
3. imposing controls over the quality of consumer goods to ensure they are compliant with safety requirements;
4. supervising the regulation of trade in precious stones and metals; and
5. receiving consumer complaints and processing them in line with consumer protection laws and regulations.

(i)

The **Guide to Consumer Rights and Responsibilities 2023** is a useful resource for consumers, providing a simplified version of Saudi Arabia's consumer protection laws and regulations to aid people's understanding of consumer-merchant transactions and rights.

(ii)

Commentary

Cloud Policy

https://www.mcit.gov.sa/sites/default/files/cloud_policy_en.pdf (i)
https://nca.gov.sa/ar/ccc-en.pdf (ii)

The Saudi Ministry of Communications and Information Technology **KSA Cloud First Policy** (2020) mandates that governmental entities (defined in the "Scope of the policy" section) prioritize cloud computing services when making new IT investment decisions, with the goal of accelerating cloud adoption. The private sector is also encouraged to create its own internal cloud-first policy.

(i)

The Saudi Arabia National Cybersecurity Authority published the Cloud Cybersecurity Controls **(CCC – 1: 2020)** which was developed to minimize the cyber security risks of Cloud Service Providers (**CSPs**) and Cloud Customers, also known as Cloud Service Tenants (**CSTs**) and highlights the Kingdoms early commitment to Cloud Services.

(ii)

Data / Privacy

https://sdaia.gov.sa/en/Research/Pages/DataProtection.aspx

The Saudi Data & AI Authority (**SDAIA**) is the main authority responsible for governing data protection in Saudi Arabia. One of the primary objectives of the SDAIA is to "*implement the best global practices for national data management and governance policies and controls, protect personal data and increase the value learned from it in order to make strategic decisions, anticipate the future and uphold the highest standards of accountability and transparency*."

The Saudi Personal Data Protection Law (**PDPL**) came into effect on 14 September 2023 and aims to regulate the handling of personal data, ensuring privacy and protection of individuals' rights, with a focus on data *minimization*, purpose *limitation* and data *subject rights.*

Fraud

https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/de92c064-d09e-4c61-89cc-a9a700f1b471/2 (i)
https://rulebook.sama.gov.sa/en/6-reporting (ii)

The **Anti-Commercial Fraud Law, 2008** seeks to protect consumers in Saudi Arabia and ensure fair trading practices within the Kingdom. Some of the Law's main features include:

- **Combatting deceptive practices** – this includes the misrepresentation of products, false advertising and the sale of counterfeit goods.
- **Setting regulations** regarding product standards and specifications – preventing the sale of products that are harmful or unsafe.
- **Adapting** to emerging commercial fraud practices – including those taking place online.

(i)

Financial crimes such as fraud should be reported to the nearest local police station and a copy of the police report must then be submitted to the **Financial Crimes Department at the Banking Supervision Division of SAMA.**

(ii)

Commentary

Sanctions

http://www.leagueofarabstates.net/ar/legalnetwork/Pages/typicalarablaws.aspx

Saudi Arabia does not have its own distinct sanctions regime. However, it adheres to sanctions imposed by both the United Nations and the Arab League (see URL).

Terrorism

https://www.aml.gov.sa/en-us/RulesAndRegulations/Combating%20Terrorism%20and%20Financing%20of%20Terrorism%20Law.pdf (i)
https://www.moi.gov.sa/wps/portal/Home/Home/!ut/p/z1/04_iUlDgAgP9CCATyEEmKOboR-UllmWmJ5Zk5ucl5uhH6EdGmcVbBro7e3iYGHm7GzqaGTh6mhv5G3iaGrp7Gul76UfhVxCcmqdfkB2oCABPX762/ (ii)

The main law governing the financing of terrorism in Saudi Arabia is the **Law on Combatting the Financing of Terrorism.** Some of the main areas covered in the Law include:

- **Preventative measures** to be carried out by financial institutions and designated non-financial businesses and professions
- **Powers of relevant regulatory authorities** i.e. investigating, prosecuting, freezing and seizing assets etc.
- **International commitments** e.g. aligning with the FATF's 40 Recommendations

The **General Directorate of Financial Intelligence** plays a key role in implementing Saudi Arabia's counter-terrorist financing regime. They are responsible for receiving and analysing suspicious transaction reports and disseminating the results to competent authorities.

(i)

Saudi Arabia's **Ministry of Interior** also plays a key role in combatting terrorism. One of their key objectives is to strengthen **security partnerships with Arab nations to prevent** terrorist threats within Saudi Arabia, helping to achieve its overarching goal of maintaining **security and stability** across the Kingdom.

(ii)

Company Registrar

https://mc.gov.sa/en/eservices/Pages/ServiceDetails.aspx?sID=2 (i)
https://mc.gov.sa/en/eservices/Pages/default.aspx (ii)

The **Saudi Business Centre** offers an electronic service enabling beneficiaries to start practising commercial activities. A step-by-step guide on how to complete the **registration process** is detailed on the Ministry of Commerce website.

(i)

The **Ministry of Commerce** offers a platform for searching company information.

(ii)

Commentary

Access to Public Information

https://my.gov.sa/en/content/information-policy (i)
https://sdaia.gov.sa/ar/SDAIA/about/Documents/Open%20Data%20Policy.pdf (ii)

The **Freedom of Information Policy** provides a legal framework for individuals requesting access to public sector information, outlining the obligations of public sector entities in handling those requests. The Policy applies to all "unprotected and open data, regardless of its source, form, or nature, to improve the performance and efficiency of work."

(i)

The process for **requesting access** or obtaining public information requires individuals to submit a **"public information request form"** – in an electronic or paper format – to the public entity in possession of the information.

The **National Data Governance Policies,** issued by the Saudi Data & AI Authority (**SDAIA**) document outlines the request and approval process in further detail.

(ii)

Other

https://www.my.gov.sa/wps/portal/snp/servicesDirectory (i)
https://istitlaa.ncc.gov.sa/en/Pages/default.aspx (ii)

The official national portal of the KSA Government.

(i)

The Istitlaa platform is a digital channel affiliated with the National Competitiveness Center, focused on gathering public, governmental and private sector feedback on proposed eco-nomic and development laws and regulations.

(ii)

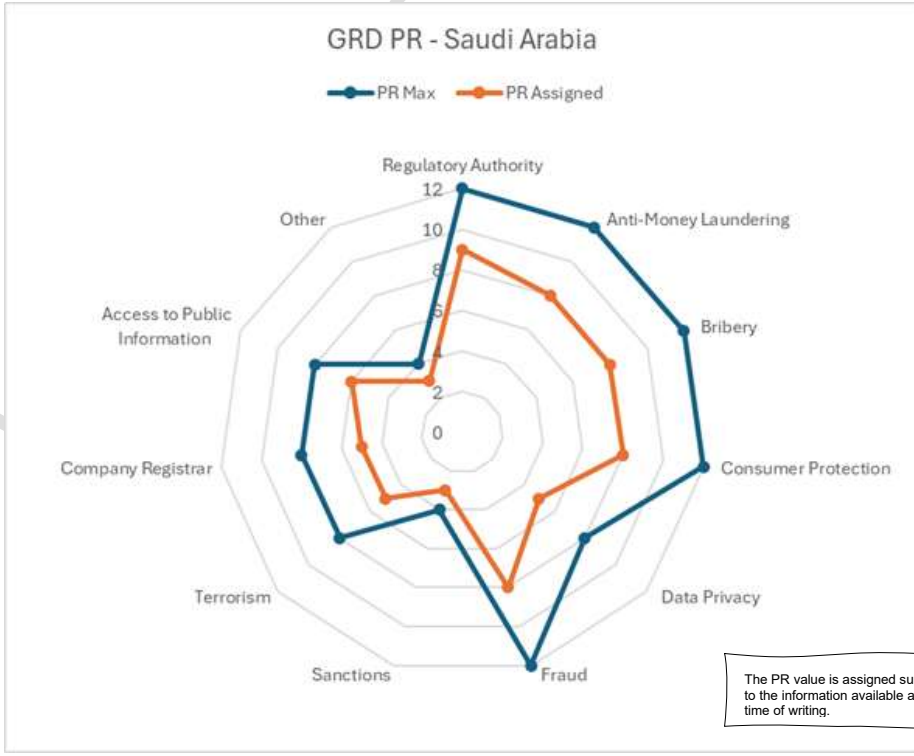
Posture Rating Saudi Arabia

The PR value of **6.8** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	9	8	8	8	5	8	3	5	5	6	3

Saudi Arabia has established many published laws and supporting ministries to ensure enforcement. However, there is currently a lack of unified digital channels, as reflected in the assigned value.

NB: **The figure does not reflect the execution of any laws, regulations or processes**



Singapore

Commentary

Financial Regulatory Authority

https://www.mas.gov.sg/

The Monetary Authority of Singapore (**MAS**) is Singapore's central bank and integrated financial regulator.

As **central bank**, the MAS manages Singapore's exchange rate, official foreign reserves and liquidity in the banking sector.

As an **integrated financial supervisor**, the MAS is responsible for well-functioning financial markets, sound conduct and investor education and regulates financial institutions in the banking, capital markets, insurance and payments sectors

The MAS, as the **central monetary authority** for Singapore, is responsible for:

1. Conducting monetary policy
2. Issuing currency
3. Overseeing the payment systems
4. Acting as a banker and financial agent to the Government
5. Delivering services and financial stability surveillance
6. Managing the foreign reserves

The official currency of Singapore is the Singapore **dollar.**

AI Act / Policy

https://go.gov.sg/nais2023 (i)

https://www.smartnation.gov.sg/sn2/ (ii)

In 2019, Singapore unveiled their first National AI Strategy, outlining plans to deepen the use of AI to transform the economy and subsequently in 2023 launched the Singapore National AI Strategy 2.0 **(NAIS 2.0)**.

(i)

The Smart Nation Program is a nation-wide effort led by the Ministry of Digital Development and Information (MDDI) to build a thriving digital future for its citizens.

(ii)

Anti-Money Laundering

https://www.mas.gov.sg/regulation/anti-money-laundering

The **MAS** is responsible for implementing measures with regards to combating financial crime in Singapore, including money laundering.

Singapore also co-chairs the Financial Action Task Force's **(FATF) Policy Development Group** and were a founding member of the **Asia/Pacific Group on Money Laundering.** As such, Singapore has significant influence on AML/CFT standards across the globe.

Some of the key requirements outlined by MAS for financial institutions in Singapore to adhere to are as follows:

- Maintaining up-to-date record of clients (including beneficial owners).
- Conducting regular reviews of accounts.
- Monitoring and reporting any suspicious transactions.

Commentary

Bribery

https://www.cpib.gov.sg/about-corruption/legislation-and-enforcement/prevention-of-corruption-act/ (i)

https://www.cpib.gov.sg/about-corruption/legislation-and-enforcement/cdsa/ (ii)

https://www.cpib.gov.sg/about-corruption/prevention-and-corruption/singapores-corruption-control-framework/ (iii)

The **Corruption Practices and Investigation Bureau (CPIB)** is exclusively responsible for tackling issues relating to corruption in Singapore. They maintain a '*zero-tolerance*' strategy, enshrined within four key pillars, listed below:

1. **Laws** – There are two key pieces of legislation in Singapore pertaining to anti-corruption and bribery. These are as follows:
   a. **Prevention of Corruption Act 1960**
      (i)
   b. Corruption, Drug Trafficking and Other Serious Crimes **(Confiscation of Benefits) Act 1992**

(ii)

2. **Adjudication** – Various provisions of the constitution can guarantee the CPIB full independence from the Supreme Court judiciary.
3. **Enforcement** – Swift and vigorous law enforcement with a heavy focus on deterrence.
4. **Public Administration** – A strong set of standards outlined in the Code of Conduct for Public Service.

(iii)

Consumer Protection

https://sso.agc.gov.sg/Act/CPFTA2003 (i)

https://www.cccs.gov.sg/-/media/custom/ccs/files/legislation/cpfta/list_of_unfair_trade_practices_under_cpfta.ashx (ii)

The Consumer Protection (Fair Trading) Act 2003 (most recently revised in 2021) is the primary piece of legislation in Singapore pertaining to consumer protection. The purpose of the Act is to protect consumers against unfair practices and establish further rights regarding non-contracted goods/services.

(i)

Enshrined within the act is the **'list of unfair trading practices',** which provides clear guidelines for both businesses and consumers as to what constitutes an unfair practice (full document available to download from Singapore's CCCS website).

(ii)

Commentary

Cloud Policy

https://www.tech.gov.sg/files/media/corporate-publications/FY2021/DGX%20Cloud%20Working%20Group%20Report%202021%20-%20Baseline%20Policies.pdf (i)

https://www.developer.tech.gov.sg/our-digital-journey/digital-government-exchange/files/DGX2023%20Cloud%20Final%20Report_Final%20(for%20publish)%20v2.pdf (ii)

https://www.tech.gov.sg/products-and-services/for-government-agencies/software-development/government-on-commercial-cloud/ (iii)

https://www.mas.gov.sg/-/media/mas/regulations-and-financial-stability/regulatory-and-supervisory-framework/risk-management/outsourcing-guidelines_jul-2016-revised-on-5-oct-2018.pdf (iv)

In 2018, the Government announced its **Cloud-first Strategy**- a five-year action plan to integrate most of its information technology (IT) systems to the commercial Cloud.

(i)

Singapore leads the **Digital Gov Exchange Workgroup on Cloud**. The group issued a report in 2023 with the aim of providing a general overview for government organizations (particularly working group member countries), in their approach to cloud adoption and how to implement services so they effectively serve citizens and businesses.

(ii/iiii)

The Singapore MAS Guidelines on Outsourcings.

(iv)

Data / Privacy

https://www.pdpc.gov.sg/who-we-are/about-us (i)

https://www.pdpc.gov.sg/overview-of-pdpa/the-legislation/personal-data-protection-act (ii)

https://www.pdpc.gov.sg/overview-of-pdpa/the-legislation/personal-data-protection-act/data-protection-obligations (iii)

The **Personal Data Protection Commission (PDPC)** is the main regulatory authority in Singapore responsible for handling issues regarding data protection. The commission was established in 2013 to administer and enforce the **Personal Data Protection Act (PDPA) of 2012** (most recently amended in 2021).

(i)

The main objectives of the PDPA are as follows:

1. Provide a coherent framework for individuals and businesses to ensure personal data rights are protected.
2. Recognising the need of organizations to collect, use or disclose personal data for legitimate purposes.
3. Strengthen Singapore's global standing by positioning it as a trusted hub for businesses.

(ii)

Another key feature of the PDPA is the **Data Protection Obligations**; requirements of all organizations to safeguard personal data (full list of obligations can be found on the PDPC website).

To ensure these obligations are fulfilled, all organizations must appoint a designated **Data Protection Officer (DPO)** who is responsible for handling matters concerning PDPA compliance.

(iii)

Commentary

Fraud

https://www.mas.gov.sg/regulation/notices/notice-cmgn01-on-reporting-of-suspicious-activities--incidents-of-fraud

The Monetary Authority of Singapore (**MAS)** is the governing authority responsible for enforcing laws and regulations pertaining to fraud prevention in Singapore.

The MAS issued a **Notice in 2013 (revised in 2024**) outlining the requirements of financial entities when reporting suspicious activities and incidents relating to fraud.

The Notice stipulates that relevant entities must file a report to the MAS within 5 working days upon the discovery of any suspicious/fraudulent activity for it to be valid.

Sanctions

https://www.mas.gov.sg/regulation/anti-money-laundering/targeted-financial-sanctions/lists-of-designated-individuals-and-entities

As a UN Member State, all natural and legal persons in Singapore are expected to screen clients against the UN sanctions list before engaging in any commercial or business activity (full list available on the official MAS website).

Terrorism

https://www.mha.gov.sg/what-we-do/managing-security-threats (i)

https://www.mha.gov.sg/what-we-do/managing-security-threats/countering-the-financing-of-terrorism (ii)

The **Ministry of Home Affairs** is the main authority responsible for combatting terrorism within Singapore. Their primary objective is to maintain peace, security and harmony by enforcing a range of legislative tools.

(i)

Singapore introduced the **Inter-Ministry Committee on Terrorist Designation (IMC-TD)** to help counter the financing of terrorism. This committee is responsible for ensuring any person or entity deemed to be a terrorist has all their funds or assets frozen immediately and that they are prohibited from partaking in any dealings.

(ii)

Company Registrar

https://www.acra.gov.sg/home/ (i)

https://www.bizfile.gov.sg/ (ii)

The Accounting and Corporate Regulatory Authority (**ACRA**) is a statutory board under the Ministry of Finance of the Government of Singapore. (i)

Businesses in Singapore can be searched via the "**Bizfile**" website, a one-stop digital service portal for business registration, filing and information. (ii)

Access to Public Information

https://data.gov.sg/

Singapore's Open Data Portal allows users access to national datasets and enables third-party developers to access APIs for development in systems.

Other

https://www.gov.sg/

https://www.judiciary.gov.sg/singapore-international-commercial-court

The web portal is the official online communication platform and repository of the Singapore Government. (i)

The website of the Singapore International Commercial Court. (ii)

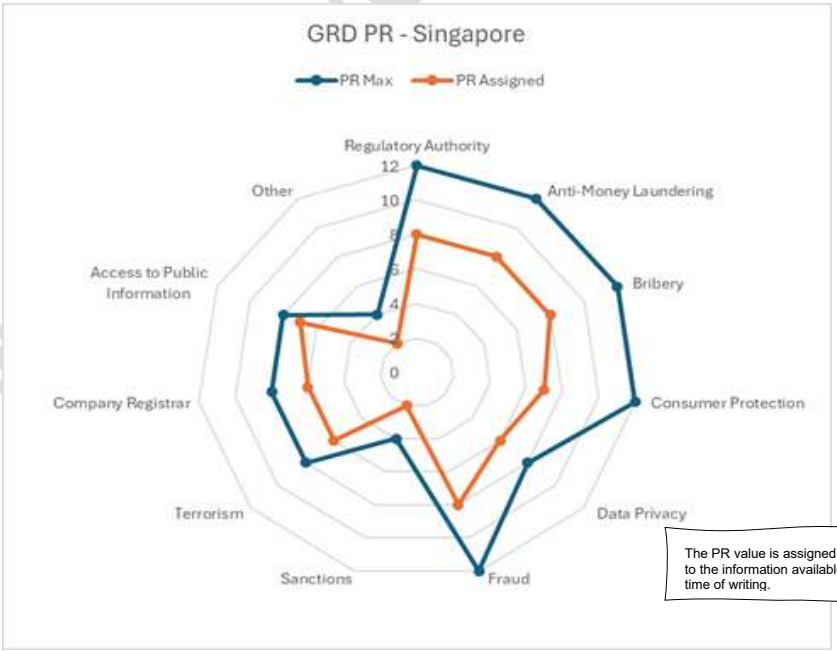
Posture Rating - Singapore

The PR value of **6.8** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	8	8	8	7	6	8	2	6	6	7	2

Singapore benefits from mature systems and processes that support compliance with the domains. However, the Monetary Authority of Singapore's wide range of responsibilities present both strengths and weaknesses. Although processes are integrated, potential conflicts in agency concerns could arise, as reflected in the assigned value.

NB: **The figure does not reflect the execution of any regulations, laws or processes**



South Korea (Republic of)

Commentary

Financial Regulatory Authority

URL

https://www.bok.or.kr/eng/main/main.do (i)

https://www.bok.or.kr/eng/bbs/E0000742/view.do?nttId=234109&searchCnd=1&searchKwd=&depth2=400066&depth3=400224&depth=400224&pageUnit=10&pageIndex=1&programType=newsDataEng&menuNo=400224&oldMenuNo=400224 (ii)

https://www.fsc.go.kr/eng/index (iii)

https://www.fss.or.kr/eng/main/main.do?menuNo=400000 (iv)

The Bank of Korea (**BOK**) is the central bank of the Republic of Korea and serves the purposes of stabilizing the value of the national currency, promoting soundness of the banking and credit systems as well as developing the Korean economy.

(i)

The BOK **Monetary Policy in Korea (Fourth Edition)** Publications.

(ii)

The Financial Services Commission (**FSC**) is a government agency with the statutory authority over financial policy and regulatory supervision. The FSC's functional responsibilities are shared among the Securities and Futures Commission (**SFC**) and subordinate bureaus and ultimately responsible for *formulating* financial policies, *supervising* financial institutions and financial markets, *protecting* consumers and *advancing* Korea's financial industry.

(iii)

The Financial Supervisory Service (**FSS**) has the primary responsibility for rulemaking and licensing while the FSS principally conducts prudential supervision, capital market supervision, consumer protection and other oversight and enforcement activities as delegated or charged by the FSC.

(iv)

The currency in use is the Korean Republic **won.**

AI Act / Policy

URL

https://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_R2V4H1W1T2K5M1O6E4Q9T0V7Q9S0U0

The AI Basic Law, also known as the **South Korean AI Act** (**SKAIA**), will take effect as of January 2026 and aligns with European principles by embedding guidelines for *human rights, human dignity and societal well-being*, while promoting competitiveness.

The SKAIA focuses on three main developmental areas:

1. **Launching** of an organizational system, including that of a National AI Committee and an AI Safety Research Institute.
2. **Supporting** measures for AI development.
3. **Establishing** mechanisms to ensure safe and reliable bases for high-risk and generative AI.

The URL links to the South Korean Basic Bill on the Development of Artificial Intelligence and the Creation of a Foundation of Trust (Alternative) (Science and Technology Information, Broadcasting and Telecommunications Committee) and only available in Korean.

Commentary

Anti-Money Laundering

https://www.kofiu.go.kr/eng/policy/amls01.do (i)
https://www.kofiu.go.kr/eng/legislation/legislation.do (ii)

South Korea's AML Regime is a comprehensive framework that encompasses legal and financial systems alongside international cooperation, serving to detect and prevent domestic and international money laundering.

The Korean Financial Intelligence Unit (**KoFIU**), established according to the Financial Transaction Reports Act (**FTRA**), plays a central role in implementing the AML Regime.

The KoFIU currently sits within the Financial Services Commission (**FSC**) and is comprised of experts from the:

- Ministry of Justice (**MOJ**)
- National Police Agency **(NPA**)
- National Tax Service (**NTS**)
- Korea Customs Service (**KCS**)
- Financial Supervisory Service (**FSS**)

The KoFIU acts as a **link between Financial Institutions (FIs)** and **law enforcement agencies,** receiving suspicious transaction reports, analysing them and disseminating them to the relevant law enforcement agencies for further examination.

On an **international level**, the KoFIU handles cross-border movements of criminal proceeds through an **Information System**, built in November 2002. The Information System allows the KoFIU to identify individuals involved in money laundering by analyzing foreign transaction reports and financial information.

Amongst its other duties, the KoFIU provides **regular training to FIs** across the nation and participates in **global networking projects**. (i)

The primary law governing money laundering in South Korea is the **Proceeds of Crime Act (POCA)**. This law criminalises money laundering, mandating the government to preserve and confiscate criminal proceeds. N.B. A full version of the Law is not currently accessible online. (ii)

Bribery

https://elaw.klri.re.kr/eng_service/lawView.do?hseq=28627&lang=EN (i)
https://www.acrc.go.kr/menu.es?mid=a20201010000 (ii)

Bribery is criminalised in South Korea under the **Criminal Act of 2013**. The Act covers a range of bribery offences, including:

- **Article 129** – Acceptance of a bribe and advance acceptance
- **Article 130** – Improper action after acceptance of a bribe and subsequent bribery
- **Article 132** – Acceptance of bribes through good offices
- **Article 133** – Soliciting a bribe (i)

The Anti-Corruption & Civil Rights Commission (**ACRC**) is the primary authority responsible for combatting bribery and corruption in South Korea. Their main functions include:

1. **Operating as a government wide cooperative system** to push forward the government's anti-corruption measures in a unified manner
2. **Creating a culture of integrity** and evaluating and measuring the public institutions' efforts and procedures to implement integrity policies
3. **Targeting corruption prone areas** e.g. by implementing fact-finding surveys, institutional improvements and follow-up inspections
4. **Operating the Anti-Corruption Training Institute** which specialises in supporting mandatory integrity education for public servants and spreading a culture of integrity into the private sector (ii)

Commentary

Consumer Protection

https://elaw.klri.re.kr/eng_service/lawView.do?hseq=49238&lang=ENG (i)
https://www.kca.go.kr/eng/sub.do?menukey=6023 (ii)
https://www.kca.go.kr/eng/sub.do?menukey=6005 (iii)

The primary law governing consumer protection in South Korea is the **Framework Act on Consumers, 2018.** The main objectives of the Act are as follows:

1. Define consumer's **rights and responsibilities**
2. Outline the **responsibilities of the State**, local governments and businesses
3. Highlight the **role of consumer organizations** and define the relationship between consumers and business entities in a free market economy
4. Establish basic principles necessary for comprehensively facilitating **consumer policies**
5. Contribute to the improvement of consumer's lives and the development of the national economy

(i)

There are also various other laws pertaining to consumer protection in South Korea, as listed on the **Korea Consumer Agency's (KCA) website** under its *'Consumer Guide'*.

The KCA is the main regulatory authority in South Korea responsible for ensuring the protection of consumer's rights. Their main functions are as follows:

1. Consumer counselling and dispute settlements
2. Policy research and recommendations
3. Collection and assessment of safety information
4. Product testing and inspections
5. Improving transaction policies
6. Consumer education/training
7. Publication and information provision

(ii)

The KCA is a member of the International Consumer Protection & Enforcement Network (**ICPEN**), which is composed of major consumer protection enforcement organizations of OECD countries. As such, they offer cross-border consumer dispute resolutions. Consumers wishing to make a complaint can do so by completing a **consumer complaint form** (available to download from the KCA website).

(iii)

Cloud Policy

https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&pageIndex=&bbsSeqNo=42&nttSeqNo=551&searchOpt=ALL&searchTxt=

At the time of writing the South Korean Ministry of the Interior and Safety (**MOIS**) announced its third "Basic Plan for Cloud Computing Promotion in the Public Sector" (the "Basic Plan"). The third basic plan for cloud computing (2022~2024) was formulated to accelerate digital innovation in all areas of the public sector and industries – see new announcement.

Data / Privacy

https://pipc.go.kr/eng/user/itc/itc/greetings.do (i)
https://pipc.go.kr/eng/user/lgp/law/lawDetail.do#none (ii)
https://www.privacy.go.kr/front/main/main.do (iii)

Personal Information Protection Commission (**PIPC**) is an independent data protection authority, responsible for formulating policies on data privacy and supervising the application of the data protection law. Some of their other functions include:

- **Handling complaints** and conducting remedial procedures
- Engaging in **international exchanges** and cooperation with foreign privacy organizations
- **Conducting research** on laws, policies, systems and practices (i)

The **Enforcement Decree of the Personal Information Protection Act** (most recently updated in 2023), is the primary law governing data protection in South Korea. The main features of the Act include:

1. Outlining the responsibilities of **Personal Data Controllers**
2. Establishing the **rights of data subjects**, e.g. the right to access, correct, delete and suspend the processing of their personal information
3. Regulations of data processing and security
4. Specifying the **Powers and duties of the PIPC** to oversee and enforce the data protection law
5. Making **provisions for nuanced cases** e.g. the processing of sensitive personal information, such as criminal records and health information (ii)

The **Personal Information Protection Portal** is a tool for individuals seeking information regarding their rights as a data subject. The Portal offers a range of services, including guidance on how to **report data protection violations.**

(iii)

Commentary

Fraud

https://www.clean.go.kr/menu.es?mid=a20106010000 (i)
https://www.clean.go.kr/menu.es?mid=a20103000000 (ii)

South Korea's Anti-Corruption and Civil Rights Commission (**ACRC**) is responsible for implementing both **preventative and reactive measures** in relation to combatting corruption and fraud. These include:

1. Conducting Integrity Assessments
2. Conducting Corruption Risk Assessments
3. Managing the Code of Conduct for Public Officials
4. Providing Anti-Corruption Training
5. Handling Corruption Reports
6. Detecting & Handling Violations of the Code of Conduct
7. Protecting & Rewarding Whistleblowers (i)

The Clean Portal is a digital anti-corruption platform, launched by the ACRC. The Portal offers a range of services for individuals seeking support on matters related to corruption and fraud. These are as follows:

1. **Information** on relevant anti-corruption and fraud laws and institutions
2. **Consultation services** to those wishing to submit a violation report
3. Guidance on **how to make reports** and signposting the relevant links to do so
4. Access to **anti-corruption materials** e.g. policies, reports, statistics etc.
5. A platform to check the results of a consultation or report (ii)

Sanctions

https://www.kofiu.go.kr/eng/policy/ptfps02_1.do

The **Financial Services Commission (FSC)** is responsible for implementing South Korea's sanctions regime.

The FSC may **designate restricted persons** on the following grounds:

- Preventing the financing of terrorism
- Implementing international treaties
- Contributing to global peace efforts

As stipulated in the "**Regulations on the Designation/Revocation of Persons Subject to Restrictions on Financial Transactions, etc.**", any individual, legal persons, or organizations designated by United Nations Security Council Resolution **1267/19889/2253, 1718, 2231, 1988** and successor resolution and Sanctions Committee formed according to the resolution are automatically designated as a person subject to restrictions in Korea.

Commentary

Terrorism

https://www.law.go.kr/LSW/eng/engLsSc.do?menuId=2&query=ACT%20ON%20COUNTER-TERRORISM%20FOR%20THE%20PROTECTION%20OF%20CITIZENS%20AND%20PUBLIC%20SECURITY#liBgcolor0 (i)

https://www.law.go.kr/lsInfoP.do?lsiSeq=182070&urlMode=engLsInfoR&viewCls=engLsInfoR#EJ5:0 (ii)

The Government of South Korea enacted the **Act on Counterterrorism for the Protection of Citizens and Public Security** with the aim of safeguarding national and public security from terrorist threats, outlining counter-terrorism activities and establishing provisions for compensation related to terrorist acts. The government body in charge of overseeing the implementation of the Act is the **National Intelligence Service.**

The Act sees the establishment of two counter-terrorism bodies:

- The **National Counterterrorism Committee** – responsible for formulating and assessing policies concerning counter-terrorism activities.
- The **National Counter-Terrorism Centre** – comprised of public officers under the jurisdiction of the Prime Minister, the Centre is responsible for coordinating and implementing the country's counter-terrorism efforts.

(i)

The **Act on Prohibition Against the Financing of Terrorism** is the primary law governing the financing of terrorism in South Korea. Some of the Act's main features include:

1. **Regulations on financial transactions** – this includes procedures for objections to designations or rejections of transaction permissions.
2. **Powers and functions of the FSC** concerning overseeing and regulating financial transactions related to terrorism financing.
3. **Implementation of international standards** – the primary purpose of the law is to implement the International Convention for the Suppression of the Financing of Terrorism and the United Nations Security Council resolution, etc.

(ii)

Company Registrar

https://englishdart.fss.or.kr/

The Repository of Korea's Corporate Filings (**DART**) website provides the capability to perform company searches.

Commentary

Access to Public Information

https://www.law.go.kr/LSW/eng/engLsSc.do?menuId=2&query=ACT%20ON%20COUNTER-TERRORISM%20FOR%20THE%20PROTECTION%20OF%20CITIZENS%20AND%20PUBLIC%20SECURITY#liBgcolor1 (i)

https://www.open.go.kr/com/main/mainView.do (ii)

The **Official Information Disclosure Act of 2001** (most recently amended in 2020), establishes a legal framework for public access to information held by government bodies. The Act aims to promote transparency by establishing clear procedures for citizens to access information and mandating the disclosure of such information.

(i)

South Korea's Information Disclosure Portal facilitates the disclosure of information held by public institutions, providing information from a range of sectors, including health, the economy and education. The Portal also enables verified users to **request access to information** that hasn't already been publicly disclosed.

(ii)

Other

https://www.gov.kr/portal/foreigner/en/m010501

The gov.kr website serves as a comprehensive source of information regarding South Korean government policies, initiatives and activities, offering access to data from various government ministries and agencies.

Posture Rating - South Korea

The PR value of **7.2** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	8	8	8	9	7	9	2	6	6	7	2

South Korea has established a set of mature systems and processes to support compliance within the domains. However, various sanctions lists are published in Korean which made analysis for non-native speakers and reflected in the assigned value.

NB: **The figure does not reflect the execution of any processes, laws or regulations.**

Switzerland

Commentary

Financial Regulatory Authority

https://www.snb.ch/en/ (i)
http://www.finma.ch/ (ii)

The Swiss National Bank (**SNB)** conducts Switzerland's monetary policy as an independent central bank.

The main responsibility of the SNB is to fulfil its monetary policy mandate (which it does independently of the Swiss Government). The three main elements of this mandate are as follows:

1. **Defining price stability**- the SNB outline price stability as a rise in the Swiss consumer price index (CPI) of less than 2% per year
2. **Medium-term inflation forecasts** – the bank publishes conditional forecasts for inflation over a 3-year period. These forecasts serve as the main indicator when informing monetary policy decisions
3. **Setting the SNB policy rate** – to facilitate price stability, the SNB aims to keep the SNB policy rate in line with the secured short-term Swiss franc money market rates

Switzerland is a small open economy and as such, is highly integrated with the global economy. Therefore, the SNB plays an active role in the various frameworks of international monetary cooperation e.g. the International Monetary Fund (**IMF**) and the Bank for International Settlements (**BIS**).

(i)

The Swiss Financial Market Supervisory Authority (**FINMA**) is an independent financial-markets regulator, who is responsible for ensuring that Switzerland's financial markets function effectively.

FINMAs mandate is to supervise banks, insurance companies, financial institutions, collective investment schemes and their asset managers and fund management companies.

FINMA regulates insurance intermediaries and is charged with protecting creditors, investors and policyholders.

(ii)

The national currency of Switzerland is the Swiss **franc**.

AI Act / Policy

https://www.sbfi.admin.ch/sbfi/en/home/eri-policy/eri-21-24/cross-cutting-themes/digitalisation-eri/artificial-intelligence.html (i)
https://www.newsd.admin.ch/newsd/message/attachments/71099.pdf (ii)

Artificial Intelligence (AI) was at the forefront of the **Digital Switzerland Strategy, 2018,** published by the Federal Council. One notable change in the 2018 strategy was the introduction of an interdepartmental working group (**IDWG**). This group's main purpose is to assess how well-positioned Switzerland is to deal with the challenges of AI, thus helping to guide policy decisions.

(i)

Due to being outside of the EU, Switzerland can set its own legislative priorities for AI. The **AI IDWG report of 2019** provides a set of rules and standards for Switzerland to follow with regards to AI regulation. At present, there are some tensions between Switzerland's current approach and those set out in international regulatory framework, which has led to increasing pressure on Switzerland to consider AI regulation in international forums. (ii)

Commentary

Anti-Money Laundering

https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-90145.html

As of January 2023, the Federal Council enforced the newly revised **Anti-Money Laundering Act (AMLA)** and the amended **Anti-Money Laundering Ordinance (AMLO).**

Some of the key changes because of the Act's amendments include:

- Promoting transparency of associations with high levels of terrorist financing risk
- Updating of client data and suspicious activity reports relating to money laundering
- Strengthening supervision and controls for precious metals

Bribery

https://www.eda.admin.ch/content/dam/schweizerbeitrag/en/documents/Publikationen/170441-Korruption-vermeiden-EB_EN.pdf (i)

https://www.oecd.org/en/topics/anti-corruption-and-integrity.html (ii)

Switzerland's Federal Department of Economic Affairs created a comprehensive document which provides an overview of Swiss criminal law on corruption.

The bribery of a private persons comes under the Federal Law's jurisdiction, regulated by the **Unfair Competition law (UWD; Article 4a).** On the other hand, bribery of a public official comes under the jurisdiction of the **Swiss Criminal Code (StGB).**

(i)

As a signatory of the **OECD Anti-Bribery Convention, 1999**, Switzerland's implementation and enforcement of anti-bribery regulation go through rigorous monitoring by the OECD Working Group on Bribery.

(ii)

Consumer Protection

https://www.kmu.admin.ch/kmu/en/home/concrete-know-how/sme-management/e-commerce/creating-own-website/statutory-obligations-in-switzerland-and-the-eu%20.html

Switzerland does not have any direct consumer protection laws. As such, activities concerning this issue are largely governed by laws with a broader scope e.g. the **Federal Law Against Unfair Competition (LCD; RS 241)** and the **Order on the Indication of Prices (OIP; RS 942.211)**, the **EU's Directive on Consumer Rights (Directive 2011/83/EU)** and the **Directive on Electrical Commerce (Directive 2000/31/EU).**

Some of the key features regarding consumer rights within the **Swiss Code of Obligations (CO; RS 220)** are as follows:

1. Customers enter a sales contract after just one 'buy click' when purchasing from an online Swiss store.
2. Once an e-commerce order has been placed, Swiss law does not obligate the seller to provide customers with a right to cancellation.
3. Swiss law does not stipulate a maximum delivery time for online sellers.
4. Online site operators must provide clear information about their products/services as outlined in **Article 3 of The Federal Law Against Unfair Competition. (LCD).**
5. Buyers have 2 years in which they can file a warranty action in the case of a faulty/unsatisfactory product.

Commentary

Cloud Policy

https://www.edoeb.admin.ch/edoeb/en/home/datenschutz/internet_technologie/cloud.html (i)

https://www.edoeb.admin.ch/edoeb/en/home/datenschutz/arbeit_wirtschaft/datenuebermittlung_ausland.html (ii)

In accordance with **Article 9 of the Federal Act on Data Protection (FADP)**, cloud service providers and users are required to comply with the following:

- Companies offering cloud services must meet requirements set out by their customers for data processing.
- Customers using cloud services are responsible for ensuring all data processing meets data protection requirements. (i)

If the cloud services involve cross-border data disclosure, checks must be carried out beforehand to ensure legal requirements are satisfied. **Article 16 of the FADP** outlines guidance for checking the admissibility of transferring data to foreign countries. (ii)

Data / Privacy

https://www.kmu.admin.ch/kmu/en/home/facts-and-trends/digitization/data-protection/new-federal-act-on-data-protection-nfadp.html

As of September 2023, Switzerland enforced the **New Federal Act on Data Protection (nFADP)**, designed to better protect personal data and grant new rights to those concerned.

As a non-EU Member State, Switzerland does not comply with the **General Data Protection Regulation (GDPR).** However, one of the primary goals of the nFADP was to align Switzerland's data protection laws more closely with those of the EU, thus ensuring Swiss companies remain strong market competitors.

Some notable elements of the nFADP are as follows:

1. Only data of **natural persons** are covered by the legislation
2. Genetic and **biometric data** are now considered **sensitive data**
3. Introduction of the **"Privacy by Design" and Privacy by Default"** principles. This essentially means all software, hardware and services must be configured to protect data and privacy
4. Companies are now obligated to keep a **register of processing activities** (with some exceptions for SMEs)
5. The Federal Data Protection and Information Commissioner (FDPIC) must be **notified promptly** in the event of a data security breach
6. **Automated processing of personal data** now falls under the law's provision

Fraud

https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/cc/54/757_781_799/20220101/en/pdf-a/fedlex-data-admin-ch-eli-cc-54-757_781_799-20220101-en-pdf-a.pdf

In accordance with **Article 146 of the Swiss Criminal Code**, fraud is defined by any person who aims to secure an unlawful gain for themselves or another by false pretences, concealment of the truth, or intentionally reinforcing an erroneous belief.

Article 147 of the Swiss Criminal Code defines computer fraud as anyone who intentionally alters or misuses electronic data to obtain financial gain.

Commentary

Sanctions

https://www.seco.admin.ch/seco/en/home/Aussenwirtschaftspolitik_Wirtschaftliche_Zusammenarbeit/Wirtschaftsbeziehungen/exportkontrollen-und-sanktionen/sanktionen-embargos/sanktionsmassnahmen/suche_sanktionsadressaten.html

The State Secretariat for Economic Affairs (**SECO**) is the Swiss governments center of competence for economic, labour and trade matter and maintains the list of sanctioned individuals, entities and organizations.

The URL above directs users to the **free online search tool** provided by SECO.

Terrorism

https://www.admin.ch/gov/en/start/documentation/votes/20210613/federal-act-on-police-measures-to-combat-terrorism.html

In June 2021, the Swiss electorate voted in favour of the new **Federal Act on Policy Measures to Combat Terrorism (PMCT),** granting authorities the right to act against persons who pose a terrorist risk. Some measures that may be taken are as follows:

- A requirement for the person to report to the authorities.
- A potential ban from contacting specific persons or leaving the country.

In extreme cases, the person may be placed under house arrest (if approved by a court).

Company Registrar

https://www.zefix.admin.ch/en/search/entity/welcome (i)
https://www.kmu.admin.ch/kmu/en/home.html (ii)
https://traderegistry.ch/ (iii)

The Swiss Central Name Index is where individuals can register businesses in Switzerland and perform company searches.

(i)

The commercial register is a public database managed by the Cantons (the member states of the Swiss Confederation), containing the main information on “commercially managed” companies.

(ii)

The Swiss Registry Smart Portal provides the ability to search the Swiss Trade Registry and provides a full-service Portal for entrepreneurs doing business in Switzerland.

(iii)

Access to Public Information

https://www.edoeb.admin.ch/edoeb/en/home/oeffentlichkeitsprinzip/oe_bund.html (i)
https://www.admin.ch/gov/en/start/documentation/access-to-official-documents.html (ii)

Since the **Freedom of Information Act** came into force in 2006, all persons have the right to access official documents from the Swiss Federal Administration, moving away from the principle of non-disclosure. Consequently, any person has the right to inspect official documents and obtain information about their content, without having to state a specific interest or motive.

(i)

The URL for requesting access to this information can be found on the Swiss government’s official portal. (ii)

Other

https://www.admin.ch/gov/en/start.html

The official portal of the Swiss Government and Federal Council.

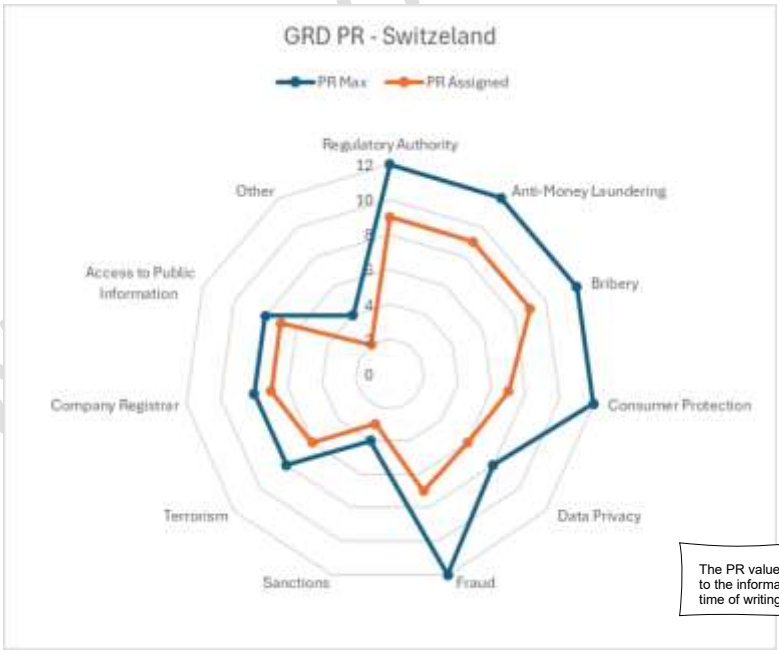
Posture Rating Switzerland

The PR value of **7.2** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	9	9	9	7	6	7	3	6	7	7	2

Switzerland has established over several decades a set of mature processes, regulations and laws which support its domains. That said, we did observe some minor deficiencies in the digital channels and the lack of unification between the Cantons and the central government channels, which is reflected in the value assigned.

NB: The figure does not reflect the execution of any policies, laws or processes in central or self-governing regional areas of Switzerland.



Thailand

Commentary

Financial Regulatory Authority

https://www.bot.or.th/en/home.html (i)
https://www.bot.or.th/en/statistics/economic-and-financial-index-and-indicators.html (ii)
https://www.bot.or.th/en/thai-economy/state-of-thai-economy.html (iii)
https://www.bot.or.th/en/our-roles/payment-systems/Payment-systems.html (iv)

The **Bank of Thailand (BOT**) is the central regulator and the chief financial regulatory authority within Thailand, with its core functions involving the supervision of the economic growth of the country, macro-economic and prudential risk initiatives as well as monitoring the frameworks in place to encourage fiscal security.

The Bank's fundamental mission and overarching strategic objective is to promote a *'stable financial environment to achieve sustainable and inclusive economic development'*; which is a core tenet of its mission statement.

(i)

In its approach to monitoring the financial health and overall condition of Thailand's economic situation, we can be directed (by the corresponding link) to the Bank of Thailand's Economic and Financial index and Indicators webpage on its website, using metrics based on a host of different factors ranging from Private Investment to Macro-Economic Indicators for growth potential. This illustrates the type of approach it must monitoring and regulating the economy of the country.

(ii)

Through the corresponding link (also on the Bank of Thailand's website), one can be directed to the press release on Thailand's economic and monetary conditions. The BOT monitors Thailand's economic conditions and presents an 'Economic and Monetary Conditions Report' on the last business day of every month, as quoted from the relevant section on its website.

(iii)

The Bank of Thailand developed **BAHTNET** (Bank of Thailand Automated High-value Transfer Network), which is a financial infrastructure to facilitate high-value funds transfer among financial institutions and organizations with current accounts at the BOT

(iv)

Thailand's currency is the **bhat**.

https://ai.in.th/en/ (i)

https://ai.in.th/en/about-ai-thailand/#:~:text=AI%20Thailand%20is%20a%20national,established.%20As%20a%20result%2C%20Thailand (ii)

The link above directs the user to the AI Thailand website, which denotes the **National AI Strategy and Action Plan for Thailand for 2022-2027**. The core objective of the National AI Strategy is to adequately and efficiently prepare essential 'infrastructure for artificial intelligence' and its uptake within Thailand and to increase Thailand's 'competitiveness' within this area and the sector. The Thailand National AI Strategy and Action Plan (2022-2027) was 'approved by the Prime Minister's Cabinet Office on July 26, 2022' as quoted on AI Thailand's website.

(i)

The ratified plan is highly methodical, segmented into five strategies and fifteen work plans. A comprehensive overview of Thailand's five Strategies within this Action Plan follows:

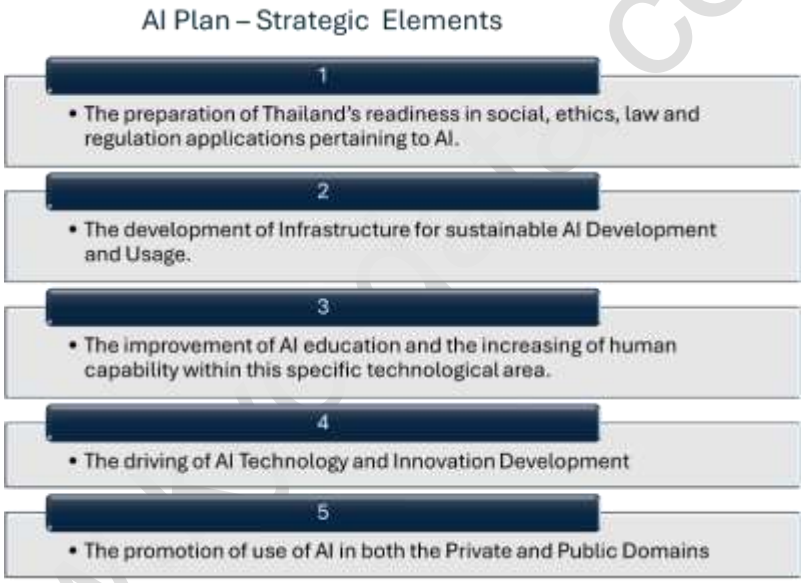


Figure 35 Thailand's Five Strategies found in the 2022 AI Plan

It is worth noting that the primary goal driving AI development and engagement is the promotion of an infrastructural ecosystem that secures Thailand's position within this globally competitive sector.

At the time of going to press the Royal Thai Police shared photos of the country's first **AI police robot** deployed in Nakhon Pathom province during a festival which was reported as having the following capabilities;

1. **Facial recognition & blacklist alerts**: identifying individuals and push a notification to officers if a high-risk individual is detected.
2. **Suspect tracking**: monitoring individuals or potential suspects across the event based on facial recognition analysis.
3. **Advanced search analysis**: perform searches across clusters or groups for individuals using facial features, clothing specifications, body types and gender.
4. **Weapon detection**: identify potential weapons including knives, wooden sticks and objects shaped or resembling weapons.
5. **Behaviour monitoring**: Analysis of interactions to detect potentially violent or disruptive behaviour, such as physical altercations or assaults.

Commentary

Anti-Money Laundering

https://cds.customs.go.th/data_files/6f86d5231634b0130986712786cfae8f.pdf (i)

https://www.amlo.go.th/amlo-intranet/index.php?option=com_k2&view=item&task=download&id=12073_37273f273ceae520c9e900dbf7ce2bac (ii)

On a domestic level, the **Anti-Money Laundering Act B.E. 2542 (1999)** is one of the primary laws governing AML in Thailand (also published by Thailand's Anti-Money Laundering Office (**AMLO**)).

(i)

It is important to note that under the "General Provisions" section of the Act (Chapter 1, S.6), there is an express provision which outlines: 'any person who commits an offense of money laundering shall, even if the offense is committed outside the Kingdom, be punished under this Act'. As such, the Act applies under the following conditions:

1. The offender/co-offenders are Thai national/s or have taken up residency in Thailand
2. The offender is foreign, but the consequence of the individual's action was intended to occur in the Kingdom, or the Thai Government is the injured party
3. The offender is foreign, but the act was perpetrated within the Kingdom's jurisdiction, provided that the person remains in the Kingdom without being extradited under international extradition law or arrangements

The **National Strategy on AML/CFT 2022-2027** was issued by the AMLO and serves two main purposes: addressing gaps in Thailand's AML/CFT/CPF action plan and ensuring it is aligned with international standards.

(ii)

Bribery

https://www.oecd.org/en/publications/oecd-review-of-thailand-s-legal-and-policy-framework-for-fighting-foreign-bribery_09fbb31d-en.html

A comprehensive overview of Thailand's generic approach to tackling bribery and other anti-corruption measures can be found on the OECD's website in a publication entitled the 'OECD Review of Thailand's Legal and Policy Framework for fighting foreign bribery'.

There are several laws and regulations regarding anti-bribery in Thailand which are illustrated below;

Figure 36 Summary of Anti-Bribery Laws in Thailand

Commentary

Consumer Protection

https://www.aseanconsumer.org/selectcountry=Thailand

The Office of the Consumer Protection Board (**OCPB**) is a government agency attached to the Office of the Prime Minister. The OCPB is primary entity/office associated with consumer affairs.

N.B. At the time of writing, the OCPB **website was unavailable.**

On the **ASEAN Consumer website**, there is relevant information relating to consumer protection law in Thailand (see URL).

The primary law governing consumer protection in Thailand is the **Consumer Protection Act 1979** (**CPA**) (most recently amended in 2019).

Cloud Policy

https://www.mdes.go.th/news/detail/8791 (i)

https://thailand.prd.go.th/en/content/category/detail/id/2078/iid/333117 (ii)

There have been several announcements regarding Thailand's **Cloud First Policy.** For instance, the Government Public Relations Department (**PRD**) outlined some key developments, including:

- Implementing the Cloud First Policy to enhance public services and efficiency
- Investments in cloud infrastructure by major tech companies
- Developing comprehensive guidelines for government cloud management, prioritizing data security and service efficiency.

(i)

The Ministry of Digital Economy and Society issued the **Law on Public Cloud Service Procurement. No. 3/2024**, which aims to provide a continuation of the development of cloud service procurement guidelines for government agencies.

(ii)

Data / Privacy

https://www.mdes.go.th/law/detail/1909-Personal-Data-Protection-Act--B-E--2562--2019- (i)

The **Personal Data Protection Act B.E. 2562 (2019**) is the primary item of legislation which governs personal data protection in Thailand.

Chapter 2, Part 1, "General Provisions" of the Personal Data Protection Act outlines the du-ties and limitations imposed on data controllers regarding the collection, use and disclosure of personal data. Specifically, Section 19 mandates that consent requests from data sub-jects must be in writing or via electronic means, unless the nature of the request makes this impossible. This highlights the importance of consent and the requirement for accessible and appropriate methods of requesting it.

Fraud

https://www.nacc.go.th/tacc/upload/files/download_201407041229342.pdf

Under **Thai Criminal Code, Section 34,** a person commits fraud by cheating when he or she obtains property from another person through deception or concealment of a fact.

Sanctions

https://www.amlo.go.th/index.php/en/

The Anti-Money Laundering Office (**AMLO**) is the government agency responsible for publishing the list of sanctioned individuals.

Commentary

Terrorism

https://www.amlo.go.th/amlo-intranet/en/files/CTF%20Act%20(consolidated%20to%20No_%202)(1).pdf (I)
https://www.amlo.go.th/amlo-intranet/media/k2/attachments/NationalYStrategyYonYAMLYCFTY-YFINAL_8380.pdf (II)

The relevant act pertaining to the countering of terrorist financing can be found on Thailand's Anti-Money Laundering Office Website and is entitled the *'Counter-Terrorism Financing Act' B.E. 2556*, the corresponding PDF outlines the Act in its entirety. (I)

The corresponding link outlines Thailand's National Strategy on Anti-Money Laundering and Countering the Financing of Terrorism 2022-2027, published by the Thai AMLO.

The strategy aimed to develop the practices and efficiencies of the previous AML/CFT regime which operated from 2017-2021.

The six primary motivations of the initial strategy were as follows;

1. To steer AML/CFT/CPF in line with international directives and standards
2. To strengthen cohesion and cooperation between all aspect of the AML/CFT/CPF framework and organizations therein
3. To promote the supervision of both the public and private agencies directed with the purpose of AML/CFT/CPF measure implementation
4. To encourage a more digitised approach regarding the country's AML/CFT/CPF Regime and to increase diversity of knowledge in this area
5. To promote AML/CFT/CPF as national agenda among the social sectors
6. To promote good governance and regulatory operations/human resources operations in this area

The new National CFT/AML/CPF regime focused on using these missions and delivering greater expediency in terms of success in these areas. Moreover, the country's re-rating in the **2018 FATF Mutual Evaluation Report Assessment**, which generated compliance concerns, necessitated the development of a new National Strategy intended to strengthen the regime and its curtailment mechanisms. (II)

Company Registrar

https://www.dbd.go.th/ (i)
https://companieshouse.co.th/ (ii)

The Department of Business Development (**DBD**), sitting within Thailand's Ministry of Commerce, is the primary custodian of business registration data. One of their main resources is **DBD Datawarehouse**, an online platform that allows users to search for companies by registration number. (i)

Companies House is a privately held Thailand company registry. The database contains every company registered in Thailand. (ii)

Access to Public Information

https://old.parliament.go.th/ewtadmin/ewt/parliament_parcy/ewt_dl_link.php?nid=16045&filename=index

Thailand's Official Information Act (**RTI Act**) guarantees the public's right to access government information. The act gives citizens the right to: Inspect official information, Request copies of official information, File complaints and appeals and ask the state to correct or change personal information.

There are **several exemptions** from free access to official information that relate to the Royal Institution, national security or international relations, law enforcement, inspections and supervisions, internal opinion and advice, life or safety of any person, right to privacy, confidential information and other cases prescribed by Royal Decree.

Other

https://www.thaigov.go.th/

The official site for the Royal Thai Government.

Posture Rating - Thailand

The PR value of **4.6** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	8	7	4	2	3	4	3	4	6	4	1

Thailand has, in most cases, defined regulations and laws to meet domain obligations. However, supporting processes and the quality of information at the time of writing resulted in low scores in some domains.

It should be noted that several URLs for government agencies resulted in dead links and thus, information was not available.

NB: The figure does not reflect the execution of laws, processes or regulations.

Türkiye

Commentary

Financial Regulatory Authority

https://www.tcmb.gov.tr/wps/wcm/connect/EN/TCMB+EN (i)
https://www.bddk.org.tr/ (ii)
https://www.cmb.gov.tr/ (iii)

The Central Bank of the Republic of Türkiye (**CBRT**) is primarily responsible for steering the monetary and exchange rate policies in Türkiye.

(i)

The core functions of the CBRT to meets its obligations under the Central Bank Law is shown below.

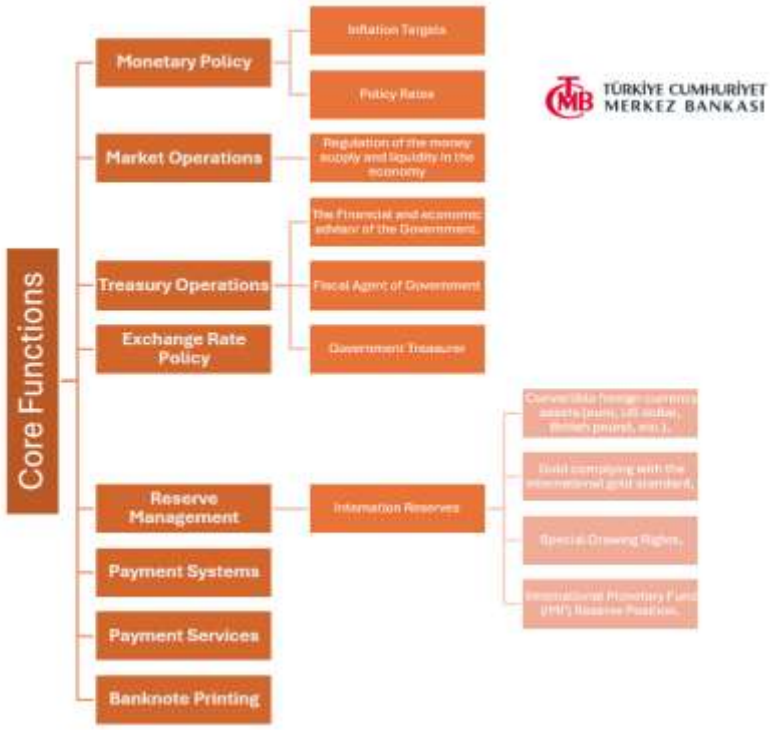


Figure 37 Core Functions of the Central Bank of Türkiye

The Bankacılık Düzenleme ve Denetleme Kurumu or Banking Regulation and Supervision Authority (**BRSA**) is responsible for the oversight and regulation of the banking sector of the Turkish financial services industry.

(ii)

Capital Markets Board of Türkiye(CMB) is the regulatory and supervisory authority in charge of the securities markets in Türkiye.

(iii)

The CBRT is the only bank with the authority to print and issue banknotes in Türkiye where the primary currency in circulation is the **lira**.

Commentary

AI Act / Policy

https://wp.oecd.ai/app/uploads/2021/12/Turkey_National_Artificial_Intelligence_Strategy_2021-2025.pdf

On 20 August 2021, the Turkish government issued the Presidential **Circular No. 2021/18** on the "National Artificial Intelligence Strategy 2021-2025" (**NAIS**).

The NAIS aims to harmonize the incentives of AI within a national context, encouraging a focus on novel technologies and developments to enhance Turkey's position in this area. The conjunction between a national plan for AI engagement with the need to understand global competition within this field has led to Turkey instilling a sense of national interest in AI developments in a domestic context.

The NAIS was first developed by the Digital Transformation Office of the Presidency of the Republic of Turkey (**DTO**). To offer some context, the NAIS was prepared in line with the **11TH Development Plan and the Presidential Annual Program for 2021**. The overarching aim of this national strategy was to concoct an agenda to harmonize the country's outlook with an agenda to create a vision for a 'Digital Turkey', engrained within the country's National Technology Initiative. By having a forward-thinking out-look and capitalising on the benefits of AI from its earlier stages, Turkey aims to be a world leader in AI Innovation.

As mentioned within the NAIS, the onus is on *'strategic compliance'* and '*end-to-end governance'* and thus implements a holistic approach in terms of AI and the ways in which it can be used. The Strategy, amongst other objectives, contains certain criteria through which it must achieve to deliver success in this area, namely;

- To have circa. 50,000 people employed within the AI space in Turkey.
- To raise the AI contribution figure to GDP to five percent
- To have Turkey included in the list of the Top 20 Countries in international AI Indices.

The NAIS, as indicated by its success metrics, prioritizes enhancing Turkey's international standing in AI, developing its AI workforce to overcome shortages and increasing the economic contribution of AI within Turkey.

Commentary

Anti-Money Laundering

https://ms.hmb.gov.tr/uploads/sites/2/2019/04/Law-No_5549-on-Prevention-of-Laundering-Proceeds-of-Crime-1.pdf (i)

https://www.fatf-gafi.org/en/countries/detail/Turkey.html (ii)

The fight against laundering proceeds of crime is directed by the Financial Crimes Investigation Board (**MASAK**), which is a main service unit of the Ministry of Finance and is directly attached to the Ministry of Finance. The requirements and obligations of entities under their supervision are articulated in the **Law on Prevention of Laundering Proceeds of Crime No. 5549**.

(i)

Turkey has been a member of the Financial Action Task Force (**FATF**) since 1991 and hence, is bound by the regulations and ordinances therein. This ensures cooperation with other members to understand and comply with their AML-CFT regimes and relevant regulations.

The country's AML-CFT regime was evaluated in the 2019 Assessment, which highlighted both areas needing enhancement and existing strengths. Prior to this, a 2018 National Risk Assessment (**NRA**) indicated a heightened risk of migrant trafficking, human trafficking and drug-related offenses due to the country's geopolitical positioning. To ensure further due diligence, a detailed follow-up process involved the country reporting to the FATF in 2021, 2022 and 2023.

Importantly, no recommendations were deemed non-compliant during this process. The 2023 follow-up report, available on the FATF website, details Turkey's compliance levels, showing full compliance in areas such as **R.9 (Financial Institution Secrecy Laws)** and **R.17 (Reliance on Third Parties).**

(ii)

Bribery

https://www.oecd.org/en/topics/sub-issues/fighting-foreign-bribery/turkiye-country-monitoring.html (i)

Bribery is and outlawed under Turkish law and regulated under Article 252 of the Turkish Penal Code (TPC) which defines Bribery as "*a benefit illegally secured directly or through intermediary by a public official or another person pointed out by a public official to perform, or not to perform, a task regarding the performance of the official's duties*." *(see "Other" domain for link to TPC).*

It should be noted that under Article 278 of the Criminal Code, a **person who fails to report an offence** to the competent authorities shall be sentenced to imprisonment for up to one year. Therefore, failure to report a bribery offence is punishable by imprisonment.

Türkiye is a Party to the **OECD Anti-Bribery Convention** and as such, is subject to rigorous peer-review monitoring over successive phases, coordinated by the OECD Working Group on Bribery.

Commentary

Consumer Protection

http://www.rekabet.gov.tr/ (i)
https://www.rekabet.gov.tr/tr/Sayfa/Mevzuat/4054-sayili-kanun (ii)

Rekabet Kurumu, (**RK**) is the Turkish Competition Authority a government agency that enforces competition law in Turkey. The RK's mission is to protect competition in the market for the benefit of consumers, businesses and the economy.

(i)

The 'Law on the Protection of Competition', also known as **Law No. 4054**, is primarily concerned with safeguarding fair market conditions. The major Article of this item of legislation would be Article 1 which outlines the generic purpose and the intention behind the law which, by and large, is to prevent 'agreements, decisions and practices which distort, prevent of 'restrict competition in the goods and services markets as well as curtailing the phenomenon of the '*abuse of dominance'* by the undertakings which dominate the market. Being a major item of legislation focused on curtailing abuse by dominance, there is also an onus on preventing monopolies as well as anti-competitive arrangements through events such as price-fixing and unfair competition policies.

(ii)

Cloud Policy

https://cbddo.gov.tr/en/public-cloud-computing-strategy/

Turkey's Public Cloud Computing Policy can be found on the Digital Transformation Office (**DTO**)) website, under the head-ing of its 'Public Cloud Computing Strategy'. It essentially underpins the value of investment in cloud computing, the need to create a more expedient IT Infrastructure system as well as the fundamental objective which is rooted in the need to 'procure the information technology infrastructure needs of public institutions from commercial cloud providers to the maximum extent possible'. Thus, there is an increased wish to engage in a strategy which optimises and maximises the efficiency of its cloud computing space.

It should be noted that Turkey started blocking VPN services along with the Tor network in 2016.

Data / Privacy

https://www.kvkk.gov.tr/Icerik/6649/Personal-Data-Protection-Law (i)
https://www.kvkk.gov.tr/Icerik/6589/o-Mission-Vision (ii)

Information regarding Turkish personal data protection law is available through the following link, which redirects users to the Turkish **Data Protection Authority's website**. The link provides details about the current legislation, including **Law No. 6698**.

Article 1 of the law outlines the law's objective: to protect individuals' fundamental rights and freedoms, particularly the right to privacy, concerning the processing of personal data.

Article 11, section 1, grants individuals the right to request information from the data controller regarding their personal data, including whether their data is processed (Art. 11.a) and matters of compliance related to this processing (Art. 11.c).

(i)

The Turkish Data Protection Authority (**KVKK**)'s mission is driven by a vision to establish Turkey and its data protection body as globally recognized and influential leaders in the field of personal data protection.

(ii)

Commentary

Fraud

The crime of fraud is regulated in Article 157 of the Turkish Penal Code (TPC) and is defined as “any person who deceives another, through fraudulent behaviour and secures a gain for himself, or others and causes loss to the victim, or another person, shall be sentenced to penalty of imprisonment for a term of one to five years and a judicial fine up to five thousand days”.

(see URL for the Turkish Penal Code in domain “Other” below).

Sanctions

URL https://en.hmb.gov.tr/fcib-tf-current-list

To address the proceeds of terror financing and the funding of terror acts through asset freezing, the ministry's website features a **Terrorist Financing (TF) list**. This list shows individuals, entities, or organizations whose assets are frozen:

1. Pursuant to the UN Security Council Resolution (within the scope of **Article 5 OF Law No.6415**);
2. Pursuant to requests from foreign countries;
3. Based on domestic freezing decisions (within the scope of **Article 7 of Law No.6415**); or
4. Within the scope of the Law on Countering Financing of Proliferation of Mass-Destruction Weapons (**Articles 3.A and 3.B of Law No.7262**).

Terrorism

URL https://ms.hmb.gov.tr/uploads/sites/2/2019/04/Law-No_6415-on-the-Prevention-of-the-Financing-of-Terrorism.pdf (i)

https://ms.hmb.gov.tr/uploads/sites/2/2019/04/R_RoM-1.pdf (ii)

Two of the key laws governing the financing of terrorism in Turkey are as follows:

- The Law on the Prevention of Financing of Terrorism No. 6415. (i)
- The Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism. (ii)

As a member of the Financial Action Task Force (**FATF**), Turkey is also subject to assessments of its actions to address the risks emanating from designated terrorists or terrorist organizations. This involves a comprehensive review of Turkey’s AML/CFT measures and their compliance with the FATF Recommendations.

(iii)

Company Registrar

URL https://mersis.ticaret.gov.tr/ (i)

https://www.ticaretsicil.gov.tr/view/hizlierisim/unvansorgulama.php (ii)

https://www.tobb.org.tr/ (iii)

Turkish law requires companies to disclose all legal ownership details to a central registry known as MERSIS. This reporting obligation applies during the initial formation of the company and when any contract amendments are made. Notably, however, the transfer of shares is not subject to this MERSIS registry requirement.

(i)

Turkish **Trade Registry** (**TR**) Gazette is published with index information of companies

(ii)

The Union of Chambers and Commodity Exchanges of Turkey

(iii)

Commentary

Access to Public Information

https://www.rti-rating.org/wp-content/uploads/Turkey.pdf (i)
https://www.amnesty.org/en/wp-content/uploads/2022/10/EUR4461432022ENGLISH.pdf (ii)

Turkey's Law on the Right to Information (**Law No: 4982**), introduced in 2004, governs access to public information.

(i)

The law was significantly altered by 40 articles of amendments in 2023, often labelled **'censorship laws.'** These changes impacted various laws, including the **Internet Law, the Press Law and the Turkish Penal Code**, most notably by criminalizing the "dissemination of false information" with potential prison sentences of one to three years – See Amnesty International's Public Statement, 2022, for further information.

(ii)

Other

https://en.hmb.gov.tr/ (i)
https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-REF(2016)011-e (ii)

While Turkey lacks a single central government website, each ministry maintains its own website, all of which are identifiable by the ".gov.tr" prefix.

(i)

URL for the "European Commission for Democracy Through Law (Venice Commission) – **Penal Code of Turkey**" document.

(ii)

Posture Rating - Türkiye

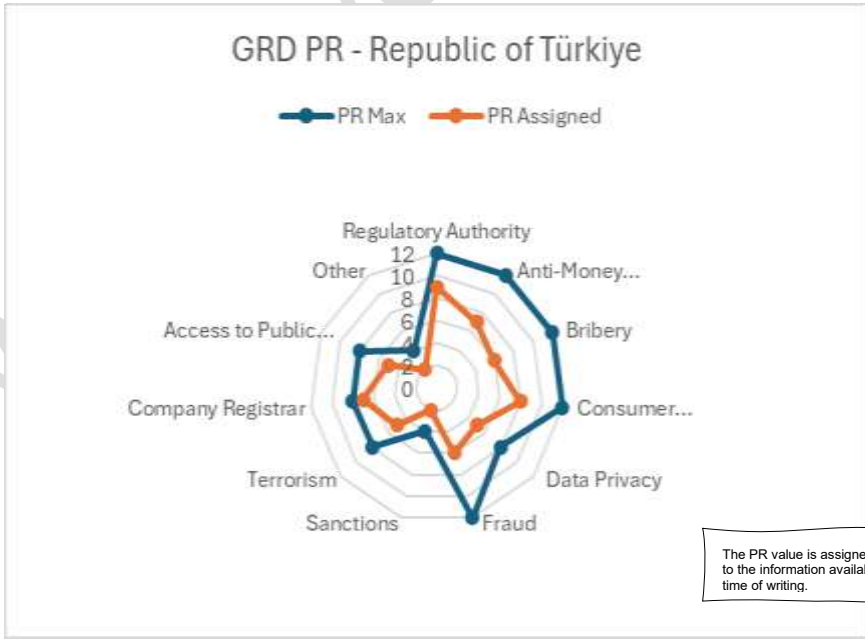
The PR value of **6.2** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	9	7	6	8	5	6	2	5	7	5	2

Whilst Türkiye has defined processes, regulations and laws to meet its obligations, the PR value reflects the available Information at time of writing.

In defining the rating, we observed several shortcomings, despite the necessary articles found in the TPC and a lack of digital tools and processes available for citizens and foreign nationals.

NB: The figure does not reflect the execution of any laws, processes and regulations.



United Arab Emirates (UAE)

Commentary

Financial Regulatory Authority

https://www.centralbank.ae/en (i)
https://rulebook.centralbank.ae/en (ii)
https://www.dfsa.ae/ (iii)
https://www.sca.gov.ae/en/home.aspx /
https://www.sca.gov.ae/assets/2f2c656d/our-philosophy-e.aspx (iv)

The Central Bank of the United Arab Emirates (**CBUAE**) is the state institution responsible for managing the currency, monetary policy, banking and insurance regulation for the United Arab Emirates. (i)

The **CBUAE Rulebook** aims to reflect the regulatory framework currently in place in the UAE. Whilst the Rulebook has **no legal effect**, it still provides the public with a broad range of regulatory information, including regulations, standards and guidelines issued by the CBUAE. (ii)

The Dubai Financial Services Authority (**DFSA**) is the independent regulator of financial services conducted in or from the Dubai International Financial Centre (**DIFC**), a purpose-built financial free zone in Dubai, UAE.

The primary objective of the DFSA is to build a clear and flexible regulatory framework. To achieve this, their stated approach is "to be a **risk-based regulator** and to avoid unnecessary regulatory burden". (iii)

The Securities and Commodities Authority (**SCA**) is a federal financial regulatory agency in the UAE, mandated by the objectives stated in the **Federal Law No. (4) of 2000.**

The SCA has three strategic objectives:

1. Building a legislative system that promotes competitiveness, attractiveness and transparency of the UAE capital market
2. Fostering transparency and investor confidence in financial markets
3. Supporting the digital transformation of businesses

(iv)

AI Act / Policy

https://ai.gov.ae/strategy/

There is no published AI strategy, at the time of writing, however information provided on the Government website define key UAE AI objectives.

The AI strategy implementation will be a multi-stakeholder effort, with cooperation from different local and federal entities within the UAE. The eight strategic objectives outlined in the AI Strategy are as follows:

1. Build a reputation as an AI destination
2. Increase the UAE competitive assets in priority sectors through deployment of AI
3. Develop a fertile ecosystem for AI
4. Adopt AI across customer services to improve government operations and quality of life
5. Attract and train talent for future jobs enabled by AI
6. Bring world-leading research capability to work with target industries
7. Provide the data and supporting infrastructure essential to become a test bed for AI
8. Ensure strong governance and effective regulation

Commentary

Anti-Money Laundering

https://www.moec.gov.ae/en/aml (i)
https://uaelegislation.gov.ae/en/legislations/1016 (ii)

Relevant information pertaining to Anti-Money Laundering and the UAE's stance on curbing financial crime in this form can be found on the UAE's Ministry of Economy's website. On the website, there is a clear outline of the measures in force to tackle illicit and illegal financial activities such as money laundering and financial sponsorship of terrorist activities.

There is a comprehensive outline of the risks which money laundering and terror financing poses to the UAE, including but not limited to:

1. **Economic recession** – considering the implication of the wider economic integrity of the UAE and the possible economic impacts of this activity
2. **Increase in crime and corruption** – the facilitation of illegal enterprise, activities and business arrangements
3. **Threats to economic stability** – volatility induced by unregulated and potentially harmful activities
4. **The weakening of financial institutions** – the undermining of the economic fabric of the UAE through the erosion of institutional control and authority

On the website, there is also organizational chart/ diagrammatic depiction of the AML-CFT Framework in the UAE.

(i)

In terms of Domestic Legislation, the Government of the United Arab Emirates has updated legislative instruments and decrees aimed at combatting terror financing, money laundering and the financing of illegal organizations.

One such example is the '**Federal Decree-Law on Anti-Money Laundering, Combatting the Financing of Terrorism and Financing of Illegal Organizations**,' which came into force on October 30, 2018. This law includes **Article 5**, which mandates the freezing of suspicious funds held by financial institutions and **Article 12**, which focuses on the development of a National Strategy to combat money laundering.

Money laundering directly threatens the UAE's economic and, to some extent, financial security. Consequently, the government prioritizes combating illicit financing and the illegal entities involved in these destructive financial activities.

(ii)

Bribery

https://u.ae/en/about-the-uae/leaving-no-one-behind/16peacejusticestronginstitutions/no-corruption-or-bribery- (i)
https://uaeaa.gov.ae/en/about/Pages/default.aspx (ii)

The UAE's Government Portal has a section dedicated to corruption and bribery, outlining the relevant Articles of the **UAE Penal Code (234-239).**

(i)

The UAE Accountability Authority is the predominant institution responsible for financial audit and accounting in the UAE.

The UAEAA focusses on safeguarding public funds be diligently outlining and monitoring the financial and operational measures and activities of the federal entities of the UAE.

(ii)

Commentary

Consumer Protection

https://u.ae/en/information-and-services/justice-safety-and-the-law/consumer-protection (i)
https://www.moec.gov.ae/en/consumer-complaints1 (ii)
https://elaws.moj.gov.ae/UAE-MOJ_LC-En/00_CONSUMER/UAE-LC-En_2020-11-10_00015_Kait.html?val=EL1&Words=2015 (iii)

Information related to consumer protection can be accessed through the United Arab Emirates' Government Portal via the following link. (i)

As specified on the Government website, the UAE has specific legal measures and protocols, as well as entities to protect consumer rights and values. Under the sub-heading **'Related E-Services'**, users can also be directed to links relating to;

- **Consumer Complaints Services** – Ministry of Economy Website
- **Requests for Consumer Complaints** – Department of Economy and Tourism (Dubai)
- **Complaints about a retailer** – Consumer Protection (Dubai).

There is also relevant information related to **Consumer Protection law**, outlining consumer rights and supplier rights. This includes a link to the relevant legislation directing consumer rights in the region. (ii)

Cloud Policy

https://www.uaelegislation.gov.ae/en/policy/details/lsy-s-lotny-llamn-lsh-by

The UAE's National Cloud Security Policy can be found on the UAE website with the onus of its mission on the creation of a forward-thinking approach to digitisation together with ensuring the protocols and measures in place, in terms of safeguarding are strong and consolidated.

The UAE's National Security Policy ensures that the principal tenet of its mission is met with direction and deliberate action, with the fundamental idea being to enhance the UAE's digital economy and cyberspace to facilitate growth in this area, both from national and a more global context.

Below is the comprehensive list of the objectives for the UAE its cloud policy mission:

1. Achieve the UAE's strategic objectives pertaining to cloud cyber security.
2. Keep up with the pace of global change and development in the field of digital economy and cyber security.
3. Safeguard and secure digital assets
4. In line with the UAE's national priority relating to Cloud Policy, strengthen cloud security and the cyberspace.
5. Accelerate the use of cloud services in the UAE by encouraging the access of government entities and businesses to relevant records and data, in line with best practice and cyber security standards.
6. Establish and maintain a successful digital ecosystem based on rigorous standards and build trust in the UAE's service providers.

Commentary

Data / Privacy

https://u.ae/en/about-the-uae/digital-uae/data/data-protection-laws

Federal **Decree Law No. 45** of 2021, also known as the **Personal Data Protection Law**, establishes an integrated framework to ensure confidentiality of information and protect the privacy of individuals in the UAE. It provides governance for data management and protection defining the rights and duties of all parties concerned.

Article 31 of the UAE's Constitution provides for *freedom of communication* by means of post, telegraph or other means of communication and guarantees their confidentiality in accordance with the law.

Fraud

https://uaeaa.gov.ae/en/core/Pages/violations.aspx?Source=/en/core/Pages/anticorruption.aspx

The UAE Accountability Authority (**UAEAA**) provides multiple secure digital channels for reporting financial corruption incidents and other financial violations and crimes to preserve confidentiality of individuals and information.

Sanctions

https://www.moec.gov.ae/documents/20121/0/CABINET+DECISION+NO+74+%281%29.pdf/dfcbee07-f90e-20e3-2e3b-52806e2a90a2?t=1655960610098

As a UN member, the UAE aligns its sanctions regime internationally, but its domestic terror list remains specific to the nation.

Terrorism

https://www.uaeiec.gov.ae/en-us/un-page?p=1

The UAE's Local Terrorist List is available via the UAE's Government portal.

The domestic list focusses on the specific sanctions against individuals from a national perspective, with the list being outlined in accordance with domestic legislation as well as the threats presented directly to the UAE.

Company Registrar

https://www.moec.gov.ae/en/company-registrars-within-the-uae

Ministry of Economy's list of company registrars within the UAE.

Access to Public Information

https://u.ae/en/about-the-uae/digital-uae/regulatory-framework/citizens-right-to-access-government-information (i)
https://u.ae/-/media/About-UAE/Digital-UAE/Guide-to-Access-Government-Information-V2017-En.pdf (ii)

The UAE Citizens' right to access government information website (i)

The UAE assures freedom and access to information through **'The Guide to Access Government Information'** and Law No. 26 of 2015 on the Organization of Dubai Data Publication and Sharing, also known as Law No. 26 of 2015: **Regulating Data Dissemination and Exchange**.

The purpose of the guide is to define core principles for accessing federal government information, thereby promoting public participation and informed understanding of governmental decisions, procedures, policies and operations affecting society. These principles can also serve as a framework for local entities, establishing access procedures within their emirates. The guide's objectives are consistent with the broader national aspirations of **Vision 2021** and the **UN Sustainable Development Goals.** (ii)

Other

https://u.ae/en (i)
https://www.mofa.gov.ae/en/the-uae/the-government (ii)

The UAE Government portal is a unified channel for governmental services. (i)

The official portal of the UAE Government . (ii)

Posture Rating – United Arabi Emirates

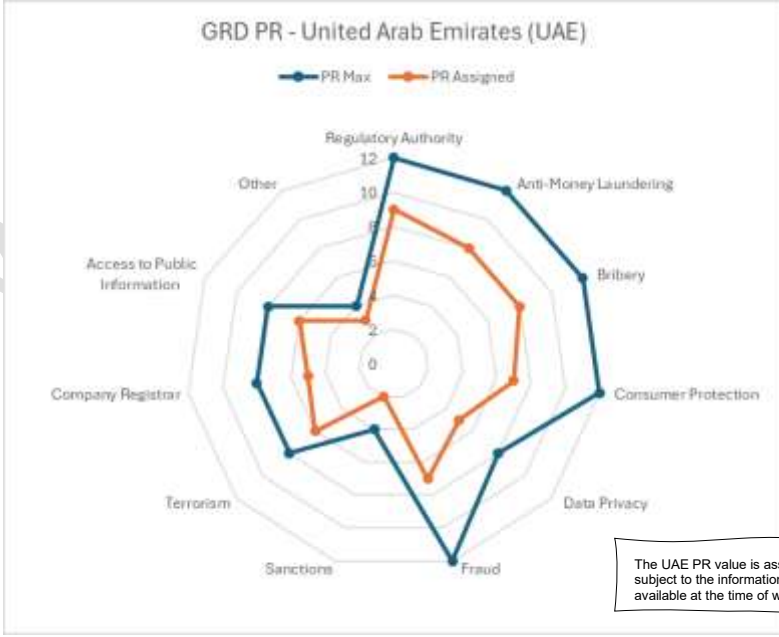
The PR value of **6.6** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	9	8	8	7	5	7	2	6	5	6	3

The United Arab Emirates and its seven emirates has adopted and defined processes, regulations and laws with strong supporting digital channels to address domain obligations.

The Central Bank Rule Book and the Portal of the UAE Government demonstrate the commitment to providing information of value to its Citizens. The value reflects the available information at time of writing excluding information presented in Arabic.

NB: The figure does not reflect the execution of laws, processes or regulations.



United Kingdom

Commentary

Financial Regulatory Authority

https://www.bankofengland.co.uk/about (i)
https://www.bankofengland.co.uk/prudential-regulation (ii)
https://www.fca.org.uk/about/what-we-do/secondary-objective (iii)
https://www.legislation.gov.uk/ukpga/2000/8/contents (iv)

The **Bank of England** serves as the United Kingdom's (UK) central bank. The Bank is owned by the Government, but in 1997 was granted operational independence over monetary policy. Some of their main duties include *maintaining financial stability and regulating banks and other financial institutions* across the country.

(i)

The Bank of England regulates and supervises UK banks, building societies, credit unions, insurers and investment firms through the **Prudential Regulation Authority (PRA).**

The PRA develops policies for regulated entities to follow, enacted through the **PRA Rulebook.** This includes ensuring financial firms have sufficient capital and adequate risk controls in place. Additionally, the PRA has authority to intervene in the activities of supervised entities where necessary to insure that they are operating in a safe and sound manner.

(ii)

The Financial Conduct Authority (FCA) was founded on April 1st, 2013. It took over conduct and regulation from its predecessor, the **Financial Services Authority (FSA)** and regulates financial activities in the United Kingdom with the aim of creating a thriving economic environment.

(iii)

The FCA is financed by the fees it charges firms. The responsibilities of the FCA are outlined in the **Financial Services and Markets Act of 2000 (FSMA).** These include:

- Protecting consumers from harmful conduct
- Maintaining the integrity of the UK financial system
- Promoting effective competition in the interests of consumers

(iv)

The UK's national currency is the Great British **pound.**

Commentary

AI Act / Policy

https://assets.publishing.service.gov.uk/media/614db4d1e90e077a2cbdf3c4/National_AI_Strategy_-_PDF_version.pdf (i)

https://assets.publishing.service.gov.uk/media/67a4cdea8259d52732f6adeb/AI_Playbook_for_the_UK_Government__PDF_.pdf (ii)

There is, at the time of writing, no general statutory regulation of AI in the UK. However, in practice various areas of law touch on AI regulation e.g. the UK data privacy regulations.

The UK's **National AI Strategy** is a 10-year plan which aims to build upon the UK's existing strengths, whilst also being a catalyst for change, utilising the power of AI to increase 'resilience, productivity, growth and innovation across the private and public sectors.'

The three main objectives underpinning the strategy are as follows:

1. **Invest and plan** for the long-term needs of the AI ecosystem e.g. working with global partners on shared research and development challenges.
2. Ensure **AI benefits all sectors and regions**. For instance, by publishing sector-specific AI strategies.
3. Effective **AI governance** e.g. determining the role of data protection in wider AI governance.

(i)

The **UK Government Guidance - AI Playbook** offers guidance for government employees and technical teams to responsibly develop, buy and implement AI to improve public services.

Recognizing the growing use of AI in the UK for applications such as weather prediction and streamlining annual car inspections (MOT). The Playbook establishes ten key principles to ensure that AI is used transparently, effectively and in the public interest.

Some of the key guidelines covered in the Playbook include;

- AI implementation should be value-driven, focusing on tangible benefits rather than mere application.
- Human oversight is essential to ensure that AI supports and does not replace decision-making.
- Public sector teams should collaborate openly, by sharing and learning from best practices.

This guidance builds on the **AI Opportunities Action Plan**, reinforcing the UK's ambition to lead in AI innovation while improving efficiency across government.

(ii)

https://www.legislation.gov.uk/ukpga/2002/29/contents (i)
https://www.legislation.gov.uk/uksi/2019/1511/contents/made?utm_source=a26d07a0-4e61-46cd-9d99-d199a74df0e5&utm_medium=email&utm_campaign=govuk-notifications&utm_content=immediate (ii)
https://www.fca.org.uk/firms/financial-crime/money-laundering-regulations (iii)
https://www.fatf-gafi.org/en/countries/detail/united-kingdom.html (iv)
https://www.legislation.gov.uk/ukpga/2000/8/contents (v)
https://www.handbook.fca.org.uk/handbook/ML/7/1.html?date=2005-04-02 (vi)

The **Proceeds of Crime Act 2002 (POCA)** is a legislative framework which primarily focuses on the recovery of criminal assets within the UK.

The Act mandates that all **regulated financial institutions and businesses** report any suspicious activity linked to criminal property or money laundering to the UK Financial Intelligence Unit (**UKFIU**). Furthermore, it also states that entities from **unregulated sectors** are obliged to report any suspicious activity they encounter in their trade, business or profession.

(i)

The **Money Laundering Regulations 2017**, subsequently amended in 2019, superseded the UK's existing Anti-Money Laundering (AML) framework. These regulations outline the obligations of financial institutions to enhance transparency and deter the manipulation of the economic system.

(ii)

The **2019 amendments** focussed on incorporating international standards set by the FATF and additionally, transposing the EU's 5th Money Laundering Directive. Some of the key changes include:

1. Requirements for firms to include new 'high-risk factors' when assessing the need for enhanced due diligence
2. Amendments to the E-money thresholds for customer due diligence
3. Duties of credit institutions and providers of safe custody services to respond to requests for information about accounts and safe deposit boxes

(iii)

The UK has been party to the **Financial Action Task Force (FATF)** since 1990 and subjected to regular assessments to review the effectiveness of UK AML/CFT measures and their level of compliance with FATF recommendations.

Since the last assessment in 2018, the FATF concluded that the UK was compliant on 24 recommendations, largely compliant on 15 and partially compliant on 1.

(iv)

As stipulated in the **Financial Services and Markets Act of 2000 (FSMA)**, the Financial Conduct Authority (FCA) (formerly known as the Financial Services Authority), is the main regulatory body responsible for enforcing AML legislation in the UK.

(v)

In accordance with the UK's Anti Money Laundering Regulations, it is mandated that all firms hire a **Money Laundering Reporting Officer (MLRO)**, responsible for combatting financial crime within companies.

(vi)

Commentary

Bribery

https://www.legislation.gov.uk/ukpga/2010/23/contents (i)
https://assets.publishing.service.gov.uk/media/5d80cfc3ed915d51e9aff85a/bribery-act-2010-guidance.pdf (ii)
https://www.gov.uk/government/publications/bribery-act-2010-post-legislative-scrutiny-memorandum (iii)

The **Bribery Act 2010** received Royal Assent on 8 April 2010. Section 7 of the Act established a new offence; commercial organizations are now criminally liable if they fail to prevent bribery by persons associated with them.

(i)

In 2011, the **Ministry of Justice (MOJ)** issued updated regulations and guidance on bribery under the Bribery Act 2010. These guidelines reflect advancements in technology and modern business practices.

(ii)

The Act criminalises both the giving and receiving of bribes within the UK. Additionally, it also criminalises the bribery of foreign public officials and outlines the obligations of organizations in the prevention of bribery.

(iii)

https://www.gov.uk/government/organisations/competition-and-markets-authority/about (i)

https://www.citizensadvice.org.uk/consumer/get-more-help/report-to-trading-standards/ (ii)

https://www.legislation.gov.uk/ukpga/2015/15/contents (ii)

https://bills.parliament.uk/bills/3453 (iv)

The **Competition and Markets Authority (CMA**) is the main regulatory body responsible for enforcing consumer protection legislation in the UK. It operates as an independent, non-ministerial department, with a primary focus on promoting competitive markets and tackling unfair behaviour. The CMA's chief responsibilities include:

1. **Investigating mergers** that have the potential to substantially harm competition
2. **Protecting individuals** from unfair trading practices, including in cases where there may be a systemic market problem
3. **Regulatory appeals** on issues such as price controls

(i)

UK citizens may also report to **Trading Standards** via the citizens advice website if they suspect or know of a business that had broken the law or acted unfairly.

Trading Standards can assist with legal matters such as taking businesses to court or prohibiting their operations, but they can't fix the problem i.e. helping consumers obtain refunds.

(ii)

The **Consumer Rights Act 2015** introduced important updates to existing consumer protection law e.g. unfair terms in contracts and faulty goods. The law also established two new regulatory areas:

1. Rights on digital content
2. Clear rules on what should happen if a service is not provided with reasonable care, skill or as otherwise agreed

(iii)

The **Digital Markets, Competition and Consumers Act 2024** empowers the **Competition and Markets Authority (CMA**) to regulate and increase competition within digital markets. Some of the key provisions within the Act include:

1. **Safeguards for consumers** against unfair commercial practices, including subscription traps, prepayment schemes and misleading savings claims.
2. **Stricter penalties** for businesses that violate consumer protection laws.

(iv)

Commentary

Cloud Policy

https://www.gov.uk/guidance/government-cloud-first-policy#full-publication-update-history

UK **Government Cloud First Policy** was published in 2017 (most recently updated in 2023).

The policy stipulates that all public sector organizations should adopt **Public Cloud** as their default choice of IT infrastructure before opting for alternatives.

Public Cloud is **mandatory** in Central Government and is strongly recommended across the wider public sector. Where Public Cloud is not possible, **community, hybrid, or private deployment models may also be considered** in certain circumstances. However, if an organization does opt for an alternative solution, they must ensure their decision is fully evidenced i.e. be able to prove that it is value for money.

The Government's **Central Digital and Data Office (CDDO)** assist organizations with spending on digital and technology related activities. The primary reason for this is to ensure that they have an appropriate mix of quality and effectiveness of hosting services across their whole life cost. This includes, capital, maintenance, operating and exit costs.

The Policy also establishes nine **Government Cloud Principles** to guide public sector organizations in implementing cloud infrastructure. The principles seek to effectively balance critical priorities; these include:

- **Speed** of technology delivery
- **Cost-effectiveness**
- **Resource** availability
- **Risk** mitigation

Commentary

Data / Privacy

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted (i)
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/data-protection-officers/ (ii)
https://assets.publishing.service.gov.uk/media/5b07eafaed915d5f767b8682/2018-05-23_Factsheet_5_-_Information_Commissioner.pdf (iii)

The **Data Protection Act** 2018 is the most consequential piece of data protection legislation governing the UK.

The Act is the UK's implementation of the EU's **General Data Protection Regulation (GDPR)**, outlining provisions for the following:

- Regulating the processing of information in relation to individuals
- Functions of the Information Commissioner
- Direct marketing codes of practice

(i)

In accordance with the UK's GDPR, all public bodies, authorities and/or groups that carry out certain processing activities must appoint a designated **Data Protection Officer (DPO).**

The main functions of a DPO are to assist in monitoring internal compliance, inform and advise on data protection obligations and serve as a primary point of contact for data subjects and the Information Commissioner's Office (**ICO**).

(ii)

As stipulated in the Data Protection Act 2018, the ICO serves as the UK's independent data protection regulator. Its main purpose is to uphold the information rights of UK citizens and as such, data controllers are obliged to inform the Commissioner of any potential data breaches which may pose a threat to an individual's rights.

Under the Act, provisions of the Information Commissioner include:

1. Enforcing sanctions in the event of a regulatory violation
2. Inspecting personal data fulfils international obligations
3. Issuing '*information*', '*assessment*' and '*enforcement*' notices where necessary to ensure data controllers are adhering to the data protection framework.

(iii)

Fraud

https://www.legislation.gov.uk/ukpga/2006/35/contents (i)
https://www.gov.uk/government/publications/fcdo-privacy-notice-fraud-and-safeguarding-investigations/fcdo-privacy-notice-fraud-and-safeguarding-investigations (ii)
https://www.gov.uk/guidance/taking-part-in-national-fraud-initiative (iii)
https://www.gov.uk/government/organisations/serious-fraud-office/about (iv)
https://www.gov.uk/guidance/fraud-statistics (v)

The UK **Fraud Act 2006** makes provisions for and in connection with, criminal liability for fraud and obtaining services dishonestly. Fraudulent acts are broken down into three categories:

- Fraud by false representation
- Fraud by failing to disclose information
- Fraud by abuse of position

(i)

The Foreign, Commonwealth and Development Office (FCDO) seeks to protect the UK's national interests through collecting, storing, sharing and using personal information.

The **Internal Audit and Investigations Directorate (IAID)** sits within the FCDO and serves as the primary point of contact for raising concerns regarding fraud, abuse and other corrupt practices. The Directorate is authorised to conduct investigations on numerous matters, primarily focusing on internal and external fraud. This includes issues concerning FCDO funds and assets.

(ii)

The National Fraud Initiative (NFI) works to detect and assist in fraud prevention by communicating data across private and public entities (including policy authorities, local probation boards and local councils).

Public sector bodies involved in the initiative must **submit data to the NFI** on a regular basis in line with specific requirements and data specifications.

In accordance with GDPR, all NFI participants must inform individuals that their data is being processed – otherwise known as a **privacy notice**.

(iii)

The Serious Fraud Office (SFO) is responsible for taking on a small number of high-profile, complex fraud cases. It is considered part of the UK criminal justice system, granted its authority from the **Criminal Justice Act 1987**.

The SFO is unique in the sense that it both *investigates* and *prosecutes* criminal cases. This is due to the complexity of the crimes they handle and hence, lawyers and investigators must work together from the offset.

(iv)

The URL Link for the publicly available fraud statistics from the Foreign, Commonwealth and Development Office

(v)

Commentary

Sanctions

https://www.legislation.gov.uk/ukpga/2018/13/contents/enacted (i)
https://www.gov.uk/government/publications/the-uk-sanctions-list (ii)
https://www.gov.uk/government/organisations/office-of-financial-sanctions-implementation/about (iii)

The **Sanctions and Anti-Money Laundering Act** (the Sanctions Act 2018) issues provisions for enabling sanctions to be imposed in the UK where appropriate. Sanctions may be imposed for several reasons, including:

- Compliance with UN obligations (or other international obligations)
- Terrorist prevention and national security
- Fulfilling foreign policy objectives

(i)

The **UK Sanctions List** publicises designated people, entities and ships in accordance with regulations outlined in the Sanctions Act 2018.

If the UK Government decides to make, vary or revoke a designation or ship specification, they will update the UK sanctions list pursuant to the **publicity provisions** in relevant sanctions regulations.

UK sanctions regimes can either be **thematic** i.e. relating to a particular issue, or **geographic** i.e. relating to a specific country or region. The full list of regimes is available on the gov.uk website and via www.kyc-data.com .

(ii)

The HM Treasury enforces financial sanctions through its **Office of Financial Sanctions Implementation** (**OFSI**).

The consolidated list of financial sanctions targets can be searched via the OFSI website.

(iii)

Different departments are responsible for implementing more specific sanctions.

Commentary

Terrorism

https://www.legislation.gov.uk/ukpga/2006/11/contents (i)
https://www.legislation.gov.uk/ukpga/2015/6/contents/enacted (ii)

Under the **UK Terrorism Act 2000**, the Home Secretary may proscribe an organization if they believe it is concerned in terrorism and it is proportionate to do so. For the purposes of the Act, this means that the organization:

1. commits or participates in acts of terrorism;
2. prepares acts of terrorism;
3. promotes or encourages terrorism (including the unlawful glorification of terrorism)
4. is otherwise concerned in terrorism.

Another significant UK terror related law is the **Counterterrorism and Security Act 2015.** This contains provisions to help the UK respond to threats of terrorism, including:

1. Disrupting people's ability to leave the country, engage in terrorist activities and then return to the UK
2. Enhancing the powers of operational agencies to monitor and control actions of those who pose a terrorist threat
3. Granting law enforcement, the authority to seize an individual's passport at the border so they can be investigated (i)

The **National Protective Security Authority (NPSA)** provides expert security advice to businesses and other relevant bodies regarding countering terrorism and other state threats. (ii)

Company Registrar

https://www.gov.uk/government/organisations/companies-house (i)
https://find-and-update.company-information.service.gov.uk/ (ii)

The UK **Companies House** is responsible for the incorporation and dissolution of limited companies. They register company information and make it available to the public. (i)

UK companies can be searched via the UK Companies House website. (ii)

Access to Public Information

https://www.legislation.gov.uk/ukpga/2000/36/introduction (i)
https://www.gov.uk/make-a-freedom-of-information-request (ii)

In accordance with the **Freedom of Information Act 2000**, all UK citizens are permitted the right to access information held by public authorities or persons providing services to them. (i)

The UK Government website provides guidance on how an individual can make a freedom of information (**FOI**) request. (ii)

Other

https://www.gov.uk/ (i)
https://www.handbook.fca.org.uk/handbook/FCG.pdf (ii)

The official website of the United Kingdom government. (i)

The **FCA's Financial Crime Guide: A firm's guide to countering financial crime risks (FCG)**, Jan 2025 offers practical help and information to firms of all sizes across all FCA-supervised sectors on how to mitigate the risk of being used for financial crime. The content mainly comes from FCA and FSA thematic reviews, supplemented with material reflecting other areas of our financial crime responsibilities. (ii)

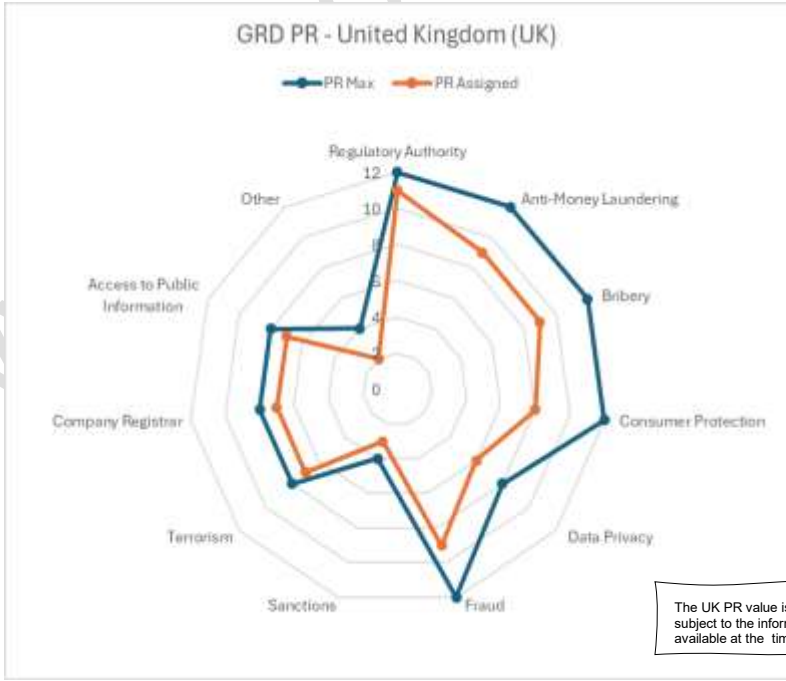
Posture Rating – United Kingdom

The PR value of **7.8** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	11	9	9	8	6	9	3	7	7	7	2

The United Kingdom has a mature set of well-defined processes, regulations and laws complemented by supporting digital channels to meet and deliver its domain and international obligations.

NB: The figure does not reflect the execution of laws, processes or regulations.



United States of America

Commentary

https://www.federalreserve.gov/aboutthefed.htm (i)
https://www.federalreserve.gov/aboutthefed/files/the-fed-explained.pdf (ii)
https://www.congress.gov/bill/96th-congress/house-bill/4986#:~:text=Depository%20Institutions%20Deregulation%20and%20Monetary%20Control%20Act%20of%201980%20%2D%20%3DTitle,unions%20to%20submit%20such%20periodic (iii)

The Federal Reserve System, otherwise known as the **Fed**, is the central bank of the United States (US). The Fed was first established in 1913 with the aim of promoting a strong and stable monetary and financial system.

(i)

There are three key system entities that make up the Fed:

- **The Federal Reserve Board –** The Board is the main governing body of the Federal Reserve System. It is comprised of 7 members, including the Chair and Vice-Chair, all appointed by the President of the US and confirmed by the Senate. The main purpose of the Reserve Board is to fulfil the goals and responsibilities of the Fed, pursuant to the Federal Reserve Act. This includes, overseeing the operations of the 12 Reserve Banks, and conducting consumer-focused research and supervision to promote fairness and transparency in the consumer financial services market.

- **The Federal Open Market Committee** (**FOMC**) – Sets the national monetary policy, with the aim of maximising employment and ensuring price stability across different geographic areas or districts in the US. The FOMC consists of 12 members, including all 7 members of the Board of Governors. They perform various functions e.g. administering interest rates, open market purchases and sales of securities. Additionally, the FMOC is responsible for directing operations within foreign exchange markets and permitting currency swaps between foreign central banks.

- **The Federal Reserve Banks –** There are 12 Federal Reserve Banks operating in total. They serve as the 'arms' of the Federal Reserve System, under the supervision of the Board of Governors. Their primary purpose is to gather data and information about businesses and local communities, helping to assist the FOMC with decisions on monetary policy. They carry out the following functions:

(ii)

The **Federal Open Market Monetary Control Act of 1980 (Monetary Control Act)** is another significant piece of legislation in relation to the US Federal Reserve System. The Act stipulates that all 'Federal and State banks, thrift institutions and credit unions must submit periodic financial reports upon the request of the Board of Governors to assist with monetary controls and credit aggregates.

(iii)

AI Act / Policy

https://www.commerce.gov/issues/artificial-intelligence (i)

https://www.nist.gov/artificial-intelligence/ai-congressional-mandates-executive-orders (ii)

https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/ (iii)

The U.S. Department of Commerce is the primary government department responsible for shaping U.S. AI policy and regulations. Two key authorities sit within this Department:

1. The National Institute of Standards and Technology (NIST), responsible for promoting innovation and building trust in how AI technologies are designed, developed, used, and governed.
2. The U.S. Patent and Trademark Office (USPTO), which focuses on incentivizing AI innovation in key emerging technologies to enhance national economic prosperity, security, and address global challenges.

(i)

The Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence **(Executive Order 14110**), enacted in 2023, originally functioned as the principal legislative framework for AI within the United States. This order has subsequently been rescinded and replaced by the Executive Order on Removing Barriers to American Leadership in Artificial Intelligence (**Order 14179**), issued in January 2025.

(ii)

The new 2025 **Executive Order on Removing Barriers to American Leadership in Artificial Intelligence** calls for an action plan to maintain and strengthen America's global lead in AI, aiming to boost human well-being, economic competitiveness, and national security. It also mandates a review of any actions taken under Executive **Order 14110** that might hinder these new goals.

Anti-Money Laundering

https://www.fincen.gov/ (i)
https://www.fincen.gov/resources/statutes-and-regulations/bank-secrecy-act (ii)
https://bsaefiling.fincen.treas.gov/AboutBsa.html (iii)
https://www.fincen.gov/anti-money-laundering-act-2020 (iv)
https://boiefiling.fincen.gov/ (v)

The Financial Crimes Enforcement Network (**FinCEN)** is the primary financial regulator in the U.S. operating under the Department of the Treasury as the country's Financial Intelligence Unit (**FIU**). Their mission is to safeguard the financial system from crimes such as money laundering and the financing of terrorism and to promote national security by working in coalition with financial authorities and effectively collecting, analyzing and disseminating financial intelligence.

(i)

FinCen is primarily governed by the Banking Secrecy Act (**BSA**) of 1970. This is a legislative framework that requires banks and financial institutions to take precautions against financial crimes, including implementing AML programmes and reporting all suspicious activities which might indicate; money laundering, tax evasion or other criminal activities.

(ii)

As of April 25, 2025, the requirement for U.S. entities (including those formerly known as "*domestic reporting companies*") and their beneficial owners to report information to FinCEN was rescinded. Furthermore, existing foreign companies required to report their beneficial ownership have an additional 30-day period in which they can do so..

(iii)

The Anti-Money Laundering Act of 2020 (**AMLA**) was passed by Congress on January 1, 2021, to amend and enhance the existing anti-money laundering (**AML**) framework. It was established under the **BSA Act of 1970.**

The AML rules aim to identify and report suspicious activities related to money laundering and terrorist financing, including securities fraud and market manipulation.

(iv)

Effective January 1, 2024, numerous companies in the United States must now report information about their **beneficial owners** – the individuals who ultimately own or control the company – to FinCEN.

(v)

https://www.justice.gov/criminal/criminal-fraud/foreign-corrupt-practices-act#:~:text=The%20Foreign%20Corrupt%20Practices%20Act,in%20obtaining%20or%20retaining%20business . (i)

https://www.trade.gov/us-foreign-corrupt-practices-act#:~:text=Under%20the%20Foreign%20Corrupt%20Practices,of%20obtaining%20or%20retaining%20business. (ii)

https://crsreports.congress.gov/product/pdf/IF/IF11588 (iii)

https://www.whitehouse.gov/wp-content/uploads/2021/12/United-States-Strategy-on-Countering-Corruption.pdf (iv)

The U.S. Foreign Corrupt Practices Act (**FCPA**) was enacted in 1977 to prevent U.S. companies from bribing foreign officials. It applies worldwide and extends to publicly traded companies.

(i)

It is against the FCPA to provide or promise to offer any form of benefit, whether directly or indirectly, to a foreign government official to retain business.

(ii)

The Securities and Exchange Commission (**SEC**) and The Department of Justice (**DOJ**) are both jointly responsible for enforcing he FCPA Act. In most instances, the authorities will settle investigations directly with companies as opposed to obtaining convictions or court judgements.

(iii)

The **U.S. Anti-Corruption Policy** complements the Strategy on Countering Corruption, aiming to institutionalise anti-corruption measures through six lines of effort. This includes expanding efforts to address new forms of corruption and providing responsive leadership during critical moments.

The above information was sourced from usaid.gov, but the website is no longer available (as of May 2025). The information has been provided here for reference only.

The **U.S. Strategy on Countering Corruption** provides a comprehensive overview of the State's approach to combatting bribery and corruption. The Strategy is formulated based on five key strategic pillars:

1. Modernising, coordinating and resourcing U.S. Government efforts
2. Curbing illicit finance
3. Holding corrupt actors accountable
4. Maintaining and strengthening existing multi-lateral anti-corruption architecture
5. Improving diplomatic engagement to help advance policy goals

https://www.ftc.gov/ (i)

https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection (ii)

https://www.consumerfinance.gov / (iii)

https://www.ftc.gov/sites/default/files/documents/statutes/credit-card-accountability-responsibility-and-disclosure-act-2009-credit-card-act/credit-card-pub-l-111-24_0.pdf (iv)

https://www.federalreservehistory.org/essays/dodd-frank-act (v)

The Federal Trade Commission (**FTC**) is the government agency dedicated to dealing with consumer protection and competition issues across a broad range of sectors within the economy.

(i)

There are several bureaus within the FTC, one of which is the **Bureau of Consumer Protection**. Their primary function is to stop unfair, deceptive and fraudulent business practices. They achieve this via various means, including:

1. Collecting information about consumers and conducting investigations
2. Developing rules to ensure fairness in the marketplace
3. Suing companies that violate consumer protection laws
4. Educating consumers and businesses about their rights and responsibilities

(ii)

The **Consumer Financial Bureau** is the government agency responsible for ensuring that consumers are treated fairly by banks, lenders and other financial institutions. They achieve this by enforcing federal consumer financial laws and holding financial service providers accountable for their actions.

(iii)

The **Credit Card Accountability Responsibility and Disclosure Act of 2009** is a key piece of consumer protection legislation in the U.S. The Law aims to protect consumers from unfair practices by credit issuers. It does so by implementing some of the following measures:

1. Enhancing disclosures to consumers
2. Limiting related fees and charges to consumers
3. Establishing constraints and protections for credit cards being issued to minors or students
4. Amending the Fair Credit Reporting Act to address fees and other terms of gift certificates

(iv)

Another significant piece of legislation pertaining to consumer protection is the **Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010.** This was primarily introduced to help tackle some of the key factors that are believed to have led to the financial crisis of 2008. Some its key features include:

1. More stringent prudential standards e.g. tougher capital, leverage and risk management requirements
2. Increasing the Federal Reserve's powers in scrutinising non-banking activities
3. More transparency in trading and the clearing of derivatives

(v)

Commentary

Cloud Policy

https://cloud.gov/strategy/

In 2019, the Office of Management and Budget **(OMB)** amended the Government's 'Cloud First' Strategy, kick-starting the transition into '*Cloud Smart'*.

The purpose of this amendment is to equip agencies with actionable information and guidance to ensure they can fully utilise the potential of cloud-computing solutions.

The Cloud Smart Strategy is founded on three key pillars:

1. **Security** – Agencies must adopt a ***risk-based approach*** when securing cloud environments. Furthermore, they must also place emphasis on data layer protections in addition to the network and physical infrastructure protections.
2. **Procurement** – Agencies must use a range of approaches to ensure they fully actualise the Government's bulk purchasing power regarding cloud technologies.
3. **Workforce** – Agencies must identify potential skills gaps that emerge because of transitioning to cloud-based solutions and provide staff with relevant training/upskilling to address these gaps.

Data / Privacy

https://www.rpc.senate.gov/policy-papers/data-privacy-in-america (i)
https://www.rpc.senate.gov/policy-papers/the-patchwork-of-federal-data-protection-laws (ii)

There is no singular data privacy law in the U.S. Instead, there are numerous Federal laws that regulate specific industries and certain types of data e.g. health data.

There is a huge amount of variation across each of the U.S. states regarding data protection. The EU's General Data Protection Regulation (**GDPR**) and the **California Consumer Privacy Act** are two of the most widely adopted laws. However, some states such as Virginia have introduced their own Acts and there are still many states with no general data protection laws at all.

(i)

A list of the various Federal data protection laws for specific industries and categories of data can be found on the Senate's official website. This includes the **Children's Online Privacy Protection Act** and the **Fair Credit Reporting Act.**

(ii)

Commentary

Fraud

https://www.justice.gov/criminal/criminal-fraud/report-fraud (i)
https://www.secretservice.gov/investigation (ii)
https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection (iii)

The Fraud Section of the Department of Justice is responsible for investigating and prosecuting complex white-collar crime cases across the United States. The Section advises on policy matters and implements enforcement initiatives.

(i)

The Secret Service was created in 1865 to combat counterfeit currency after the Civil War and has since expanded its investigative duties to protect America's financial and payment systems from criminal exploitation.

(ii)

Under the FTC, the **Bureau of Consumer Protection** aims to prevent fraudulent and deceptive business practices by enforcing laws, setting fair marketplace regulations and educating consumers and businesses about their rights and responsibilities.

(iii)

Sanctions

https://ofac.treasury.gov/#:~:text=The%20Office%20of%20Foreign%20Assets,traffickers%2C%20those%20engaged%20in%20activities (i)
https://sanctionssearch.ofac.treas.gov/ (ii)
https://ofac.treasury.gov/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists (iii)
https://www.state.gov/economic-sanctions-policy-and-implementation/ (iv)
https://www.commerce.gov/bureaus-and-offices/bis?_gl=1*151irez*_gcl_au*MTE0NzEzNzAzLjE3MDY4MDE1NDE (v)

The Office of Foreign Assets Control (**OFAC**) oversees sanctions in the USA.

(i)

OFAC generated the Sanctions List Search tool, given the number of U.S.-based sanction lists that are maintained.

(ii)

The primary sanctions list in the U.S. is the Blocked Persons List and the Specially Designated Nationals (**SDN List**).

(iii)

The Office of Economic Sanctions Policy and Implementation (**OESP**) is responsible for developing and implementing foreign policy-related sanctions. They further guide the Department of Treasury and Commerce in implementing sanctions.

(iv)

The Bureau of Industry and Security (**BIS**) is responsible for enforcing export controls and ensuring treaty compliance while promoting U.S. leadership in strategic technologies.

(v)

Commentary

Terrorism

https://www.state.gov/bureaus-offices/under-secretary-for-political-affairs/bureau-of-counterterrorism/ (i)
https://www.dhs.gov/counter-terrorism-and-homeland-security-threats (ii)
https://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf (iii)

The **Bureau of Counter Terrorism** plays a leading role in promoting U.S. national security, developing strategies and approaches to combat terrorism and securing cooperation from international partners. (i)

One of the Department of Homeland Security's (**DHS**) key priorities is to combat terrorism and protect the country from potential security threats. It achieves this by focussing on four key goals:

1. Collect, analyse and share actionable intelligence
2. Detect and disrupt threats
3. Protect designated leadership, events and soft targets
4. Counter weapons of mass destruction and emerging threats (ii)

One of the most significant pieces of legislation on terrorism in America is the **USA Patriot Act**. This was first enacted in 2001 in response to the 9/11 terror attacks and has played a crucial role in improving America's counter-terrorism efforts. Some of the measures implemented include:

1. Allowing law enforcement agencies to make use of tools already being used to investigate organised crime
2. Facilitating information sharing and cooperation between government agencies
3. Updating the law to reflect new types of terrorist threats and technologies
4. Increasing penalties for those who commit crimes relating to terrorism (iii)

Company Registrar

https://www.sec.gov/ (i)
https://www.sec.gov/edgar/search / (ii)

Registration statements, periodic reports and other forms can be accessed by typing the name or ticker symbol of a company on the Securities and Exchange Commission **(SEC) website.** (i/ii)

EDGAR advanced search gives you access to the full text of US electronic filings since 2001 based on time, type, or other categories. (ii)

Access to Public

https://www.commerce.gov/sites/default/files/opog/foia-5usc552.pdf

The Freedom of Information Act (**FOIA**) stipulates that any person has the right to obtain federal agency records (excluding those protected from public disclosure).

Other

https://www.usa.gov/ (I)
https://www.fincen.gov/boi (ii)
https://www.fincen.gov/boi (iii)

The official website of the Government of the United States. (i)

This reporting requirement has since been rescinded - for more information, see Anti-Money Laundering domain. (ii)

The US Patriot Act. (iii)

Posture Rating – United States of America

The PR value of **8.5** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	11	10	11	10	6	10	3	7	7	7	3

The United States of America (USA) has a mature, well-defined and published set of regulatory processes supported by regulations and laws to address the domains and any international obligations.

NB: The figure does not reflect the execution of any processes, laws and regulations.

The US PR value is assigned subject to the information and governmental structures in place at time of writing (May 2025).

Commentary

URL https://www.sbv.gov.vn/

According to the law relating to the State Bank of Vietnam (**SBV**) of 2010, the SBV:

1. organizes, manages and supervises the national payment system
2. provides payment services to banks
3. participates in organizing and supervising the operation of payment systems in the economy and
4. manages payment means in the economy

The main objectives of the SBV are as follows:

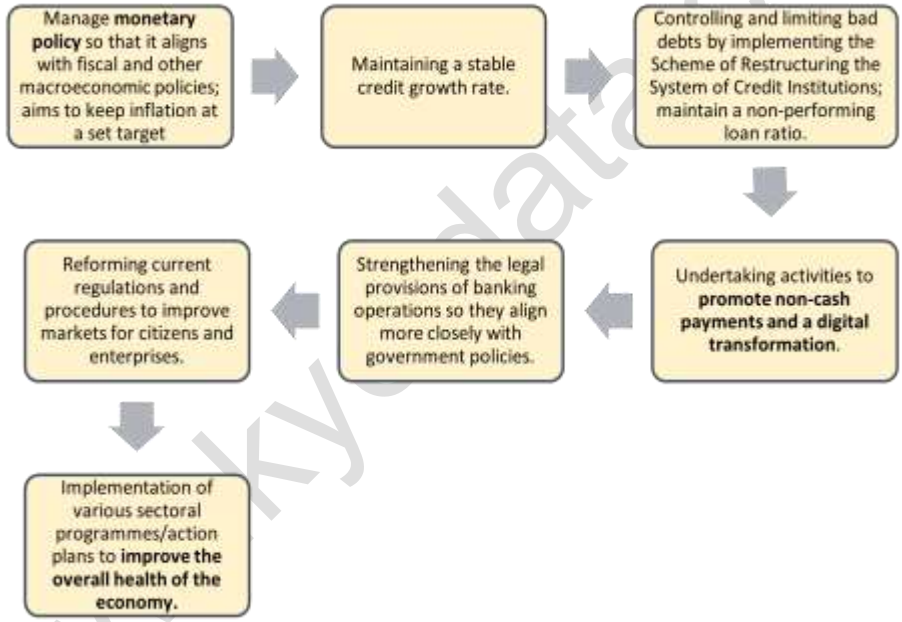


Figure 38 Objectives of the State Bank of Vietnam

The national currency in Vietnam is the **Dong** (abbreviated as 'd' in the domestic market and 'VND' in the international market).

Commentary

AI Act / Policy

https://en.baochinhphu.vn/national-strategy-on-rd-and-application-of-artificial-intelligence-11140663.htm

In January 2021, the Government of Vietnam issued the **National Strategy for Research, Development and Application of Artificial Intelligence until 2030.** The strategy is based on five key strategic pillars:

1. Implementing regulations and a legal framework in relation to AI, ensuring they meet the requirements to promote research, development and AI application in real life.
2. Creating a data and computing infrastructure to promote data sharing for AI research and increase capacity for cloud computing services.
3. Expanding the AI ecosystem, e.g., implementing training courses in AI to encourage young people into AI-centred careers.
4. Promoting AI application in business and socio-economic fields.
5. Promoting international cooperation in AI e.g. exchanging experts, improving institutions and polices to attract more foreign investment in AI.

Anti-Money Laundering

www.sbv.gov.vn/webcenter/portal/en/home/sbv/news (i)

https://apgml.org/includes/handlers/get-document.ashx?d=fe7e2cd9-c219-43a7-a4b2-f5826cf93ae3 (ii)

https://apgml.org/about-us/page.aspx?p=91ce25ec-db8a-424c-9018-8bd1f6869162 (iii)

https://apgml.org/about-us/page.aspx?p=acbf69ba-a694-4db0-b1be-f27172dde9fc (iv)

In 2022, the SBV issued an updated version of the 2012 **Law on Anti-Money Laundering.**

The law largely sets out to align Vietnamese policy on anti-money laundering (AML) more closely with international requirements and standards, developing a portfolio of legal documents with the aim of overcoming previous obstacles and shortcomings.

(i)

Vietnam is a member of the Asia Pacific Group on Money Laundering (**APG**). However, the mutual evaluation report (MER) of Vietnam was adopted by the APG in 2022 and the 1st Evaluation Report (See URL) was published in June 2023.

(ii)

The APG has various functions one of which is to facilitate mutual evaluations of all member states, ensuring compliance with international AML/CFT standards.

(iii)

Despite not being part of the FATF, as an APG Member State, Vietnam is still required to comply with many of the FATF's international AML/CFT standards, e.g., criminalizing money laundering and terrorist financing, freezing terrorist assets and implementing measures related to proliferation financing.

(iv)

Commentary

Bribery

https://vbpl.vn/TW/Pages/vbpqen-toanvan.aspx?ItemID=622&Keyword=penal%20code (i)
https://en.baochinhphu.vn/govt-adopts-national-strategy-to-combat-corruption-11123101210084819.htm (ii)

Vietnam's legal framework against bribery is enshrined within the **Penal Code (No.15/1999/QH10).** There are four key articles that outline the penalties in place for those involved in bribery and the severity of those penalties depending on various factors, e.g., amount of money involved and whether the bribe was state or privately owned. The articles are as follows:

- **Article 279**: Receiving bribes
- **Article 289**: Offering bribes
- **Article 290**: Acting as an intermediary for a bribe
- **Article 309**: Bribing or coercing an individual into making false declarations/supplying falsified documents.

(i)

Whilst there is no explicit strategy for combatting bribery in Vietnam, the Government did issue a **National Anti-Corruption Strategy** in 2022. This focussed on devolving powers to local authorities, resulting in all 63 provinces establishing provincial/municipal anti-corruption committees to help tackle the issue.

As a signatory of the **UN Convention against Corruption**, another key objective of the strategy was to align Vietnam's anti-corruption policies with the rights and obligations outlined in the convention, increasing the overall efficacy of its international cooperation regarding combatting corruption.

(ii)

Consumer Protection

https://vbpl.vn/TW/Pages/vbpqen-toanvan.aspx?ItemID=10500#:~:text=This%20Law%20regulates%20the%20rights,individuals%20trading%20goods%20and%2For

In 2011, the National Assembly of Vietnam issued the **Law on Protection of Consumer's Rights.** The main areas under this law's jurisdiction are as follows:

1. The rights and obligations of consumers.
2. The liability of organizations or individuals trading goods and/or services to consumers.
3. The liability of social organizations in protecting the interests of consumers.
4. Resolving disputes between consumers and organizations/individuals trading goods and/or services.
5. Responsibilities of the State in protecting consumer's rights and interests

Cloud Policy

https://en.baochinhphu.vn/national-strategy-on-rd-and-application-of-artificial-intelligence-11140663.htm

There is currently no standalone policy in Vietnam pertaining to cloud computing. However, development plans for cloud usage can be found within the **National AI strategy**. For example, one of the objectives assigned to the Vietnam Academy of Science and Technology is to establish a national centre for big data storage and high-performance cloud computing. This aligns closely with one of Vietnam's 2025 targets: to become a top 60 leading country in research, development and AI application.

Commentary

Data / Privacy

https://mps.gov.vn/pbgdpl/van-ban-moi/tu-0172023-bat-dau-ap-dung-quy-dinh-ve-bao-ve-du-lieu-ca-nhan-t1062.html (i)

https://mps.gov.vn/pbgdpl/van-ban-quy-pham.html?ItemId=2686#parentHorizontalTab4

Vietnam issued its first official personal data protection regulation in July 2023, **Decree No. 13/2023/ND-CP.**

Pursuant to the Decree, the governing authority responsible for protecting personal data is the Department of Cyber Security and High-Tech Crime Prevention and Control- **Ministry of Public Security (MPS).**

One of the key features of the new Decree was the introduction of the **National Portal on Personal Data Protection**. This outlines laws, policies and guidelines on personal data protection and receives notifications of any data protection violations. If the portal is notified about a violation, the MPS must take the appropriate course of action in accordance with data protection laws.

In the event of a personal data breach, **the PDPD mandates immediate notification**. The Data Processor notifies the Data Controller, who, along with the Data Controlling and Processing Party, must inform the MPS **within 72 hours**. Failure to do so requires promptly providing reasons for the delay

(i)

The full Decree can be found on the MPS's website.

(ii)

Fraud

https://vbpl.vn/TW/Pages/vbpqen-toanvan.aspx?ItemID=622&Keyword=penal%20code

There is currently no standalone legislation against fraud in Vietnam. However, there are several articles enshrined in the **Penal Code (No.15/1999/QH10)** that focus on regulating against fraud. For example, under **Article 162**, any individual who intentionally deceives a customer and causes them serious loss will be convicted of fraud.

Sanctions

https://en.bocongan.gov.vn/terrorist/terrorist-group.html

Ministry of Public Security sanctions list of terrorism-related organizations and individuals.

The Ministry of Public Security in Vietnam has designated "Vietnam Reform Revolutionary Party - Viet Tan" as a terrorist group, citing its alleged involvement in terrorist acts against Vietnam and its people, under Vietnamese and international law.

The Ministry Publishes Information about leaders of "Viet Tan" in foreign countries on its website.

Commentary

Terrorism

https://chinhphu.vn/default.aspx?pageid=27160&docid=169361 (i)

https://datafiles.chinhphu.vn/cpp/files/vbpq/2013/08/28_khungbo.pdf (ii)

In 2013, the National Assembly of Vietnam issued the **Law on Terrorism Prevention and Combat.** The primary aims of this law were to clearly define the principles, policies and measures required to combat terrorism in Vietnam. Additionally, the law clearly stipulates the responsibilities of agencies and organizations to cooperate with international regulations and requirements regarding terrorism.

(i)

The full document can be downloaded from the official information channel on Vietnam's Government Portal.

(ii)

Company Registrar

https://dangkykinhdoanh.gov.vn/en/Pages/default.aspx

The National Business Registration Portal- Vietnam's official company registrar.

Access to Public Information

https://vbpl.vn/TW/Pages/vbpqen-toanvan.aspx?ItemID=11040&Keyword=access%20to%20information

In accordance with the Law on **Access to Information 2016**, all Vietnamese citizens are guaranteed the right to access public information.

Articles 6 and 7 of the law stipulate certain instances whereby information may be inaccessible/restricted to some degree e.g. information that could harm the interests of the state.

Pursuant to Article 10 of the law, citizens may obtain access to information by the following modes:

- Freely accessing information published by state agencies
- Directly requesting information from relevant state agencies.

Other

https://vietnam.gov.vn/ (i)

https://e-services.mps.gov.vn/?home=1 (ii)

The official website of the Socialist Republic of Vietnam.

(i)

The public service portal – Ministry of Public Security – e-services in Vietnam.

(ii)

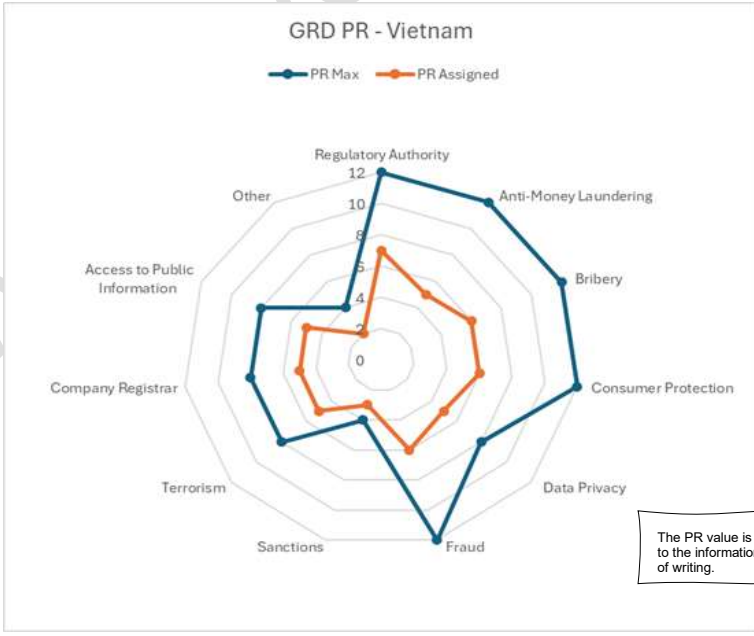
Posture Rating – Vietnam

The PR value of **5.5** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	7	5	6	6	5	6	3	5	5	5	2

Vietnam has defined many regulations and laws and supporting processes to meet its domain obligations. However, during analysis, we observed many e-services and information portals provided invalid or incomplete links when selected and was reflected in the value assigned accordingly.

NB: **The figure does not reflect the execution of any processes, laws or regulations**.



Zimbabwe

Commentary

Financial Regulatory Authority

https://www.rbz.co.zw/ (i)

https://www.rbz.co.zw/documents/mps/2025/MPS_February_06_2025_1.pdf (ii)

The Reserve Bank of Zimbabwe operates under the Reserve Bank of Zimbabwe Act, Chapter 22: 15 of 1964. The Act provides for the Board of Directors and the post of Governor who is responsible for the day-to-day administration and operations of the Bank. The Governor is assisted by two Deputy Governors.

The Governor and his two deputies are appointed by the State President for renewable five-year-terms. The board of directors is chaired by the Governor and its membership includes a maximum of seven non-executive directors, appointed by the President and representing key sectors of the economy.

(i)

The Reserve Bank of Zimbabwe's 2024 monetary policy is apprized by 2 key strategic pillars; restoring price and exchange rate stability and re-monetising the local currency. To achieve these, the bank has set out five key policy focus areas:

1. Currency and Exchange Rate Stability
2. Financial Sector Stability
3. Money Supply Growth
4. Foreign Exchange Mobilisation and Reserve Accumulation
5. Promoting Increased Demand for the Local Currency

(ii)

The local currency in Zimbabwe is the Zimbabwean **dollar.** However, the Zimbabwean economy operates under multi-currency system and as such, has seen a surge in dollarisation in recent years due to the weakening of the ZW$, with the US dollar, accounting for over 80% of market transactions in 2024.

AI Act / Policy

https://au.int/en/documents/20240809/continental-artificial-intelligence-strategy

Zimbabwe does not currently have any standalone national policies regarding AI. Having said that, in 2024, the **African Union (AU)**, which Zimbabwe is a Member State of, released the **Continental Artificial Intelligence Strategy.**

The primary purpose of the AU's AI strategy is to create a more unified approach among AU Member States regarding the implementation and regulation of AI, aiming to promote ethical, responsible and equitable AI practices.

Commentary

Anti-Money Laundering

https://www.fiu.co.zw/index.php/aml-cft-framework/ (i)

http://www.fiu.co.zw/amlcft-framework/ (ii)

The Financial Intelligence Unit (**FIU**) was established in 2004. It is part of the Reserve Bank of Zimbabwe's administrative establishment and is responsible for ensuring AML/CFT compliance.

Zimbabwe's AML/CFT framework is comprised of various pieces of legislation, including:

- The Money Laundering and Proceeds of Crime **Act [Chapter 9:24**].
- The Bank Use Promotion **Act [Chapter 24:24].**

The full list of relevant AML/CFT legislation can be found on the FIU's website.

(i)

The main **objectives of Zimbabwe's legal framework** are as follows:

1. Stipulating the powers and functions of the FIU
2. Outlining the AML/CFT obligations of financial institutions and Designated Non-Financial Businesses and Professions (DNFBPs)
3. Criminalizing money laundering and the financing of terrorism
4. Implementing the United Nations Security Council Resolution 1267 of 1999 (and its successor resolutions) and UNSCR 1373 of 2001

(ii)

Bribery

https://www.jsc.org.zw/upload/Acts/2004/0916updated.pdf (i)

https://www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf (ii)

In accordance with Chapter 9:16 of the **Prevention of Corruption Act, repealed by Act 23 of 2004**, bribery is criminalised both in the public and private sector. The Minister of Justice, Legal and Parliamentary Affairs is typically responsible for enforcing this act, although the President may also assign other Ministers where appropriate.

(i)

In 2007, Zimbabwe signed the **United Nations Convention against Corruption,** committing them to the development and implementation of effective policies to prevent corrupt behaviours e.g. bribery.

(ii)

Commentary

Consumer Protection

https://www.ccz.org.zw/wp-content/uploads/2021/07/Consumer-Protection-Act-Part-1.pdf

In 2019, the Consumer Council of Zimbabwe issued the **Consumer Protection Act (Chapter 14:14).** The purpose of this act is to protect consumers of goods and services by establishing a fair and open marketplace. Some of the key features of the act are as follows:

1. The introduction of the **Consumer Protection Commission (CPC),** which aims to enforce and protect consumer rights and promote fair business practices.
2. Establishing the rights of **consumer protection advocacy groups**, outlining conditions required for them to receive accreditation.

The provision of alternative dispute resolutions, governed by designated **consumer protection officers** (appointed by the Minister of Industry and Commerce).

Cloud Policy

https://www.ictministry.gov.zw/ (i)

https://www.ictministry.gov.zw/wp-content/uploads/2024/01/National%20ICT%20Policy%202022-2027.pdf

The Government of Zimbabwe Ministry of ICT homepage.

(i)

Zimbabwe's cloud policy is enshrined in the **National ICT Policy 2022-2027**.

(ii)

Within this policy, the ICT ministry outlines various measures to promote the use of cloud services. For example, capitalising **State Enterprises and Parastatals (SEPs),** enabling them to implement large, long-term initiatives.

To ensure data sovereignty is preserved in relation to cloud service usage, Zimbabwe issued the **Data Protection Action [Chapter 11:12] of 2021** to increase data protection and build confidence and trust in cloud service providers and users.

Data / Privacy

http://www.ictministry.gov.zw/wp-content/uploads/2024/01/Cyber-and-Data-Protection-Act-Chapter-1207.pdf (I)

https://zimlii.org/akn/zw/act/2021/5/eng@2022-03-11 (ii)

Zimbabwe's **Cyber and Data Protection Act [Chapter 12:07]** was issued in 2021, with the aim of building trust in the use of information and communication technologies.

(i)

Some key elements of the act specifically related to data protection are as follows:

1. Outlining the functions of the **Data Protection Authority** e.g. promoting, regulating and enforcing fair processing of data.
2. Dictating the rights of data subjects and obligations of data controllers.

The Cyber and Data Protection Act, 2021.

(ii)

Clearly define the **processes and penalties** in place for any data protection breaches.

Commentary

Fraud

https://www.jsc.org.zw/upload/Acts/2017/0923updated.pdf (i)
https://www.afdb.org/en/about-us/organisational-structure/integrity-and-anti-corruption (ii)

In line with **Article 136 of Zimbabwe's Criminal Law (Codification and Reform), Chapter 9:23**, fraud is considered a criminal offence, defined by any person who makes a misrepresentation intending to deceive another person, or intending to cause another person to act upon the misrepresentation.

(i)

As a member of the **African Development Bank Group (AfDB)**, the Integrity and Anti-Corruption Department's mandate also plays a key role in regulating fraudulent transactions and activities in Zimbabwe. The mandate is a multi-faceted approach to combatting fraud and other sanctionable practices, implementing measures such as risk assessments and sensitisation programs to deter such practices.

(ii)

Sanctions

https://news.un.org/en/story/2016/05/528382-un-sanctions-what-they-are-how-they-work-and-who-uses-them

As a UN Member State, Zimbabwe was subject to the UN's first sanctions regime in 1966. At present, UN is not imposing any sanctions on Zimbabwe.

Terrorism

https://zimlii.org/akn/zw/act/2007/5/eng%402016-12-31

In 2007, Zimbabwe enacted the **Suppression of Foreign and International Terrorism Act.** This repealed its previous legislation, the **Foreign Subversive Organizations Act [Chapter 11:05].**

The act serves several key purposes, including:

1. Aligning Zimbabwe's counter-terrorism regulations more closely with other international conventions e.g. the UN and African Unity's conventions.
2. Establishing the governing power of the Minster of Home Affairs in regulating against terrorist activities.

Granting the Minister of Home Affairs authority (with the President's permission), to call upon Member States of the UN to apply measures regarding foreign or international terrorist activities.

Company Registrar

https://cipz.pfms.gov.zw:8090/Auth/CipzLandingPage?ReturnUrl=%2FHome%2FIndex

Established under the Companies and Other Business Entities **Act [Chapter 24:31]**, the Companies and Intellectual Property Office of Zimbabwe (**CIPZ**) handles the registration of companies and other business entities in Zimbabwe.

Commentary

Access to Public Information

https://zimlii.org/akn/zw/act/2002/5/eng%402016-12-31

In accordance with the **Access to Information and Protection of Privacy Act [Chapter 10:27]**, all Zimbabwean citizens have the right to access public information and records held by government bodies.

For an individual to gain access to public records, they must make a formal request, in writing, to the relevant public body, providing the necessary details required to locate the information.

Other

www.zim.gov.zw/index.php/en/

The official website of the Government of Zimbabwe.

Posture Rating – Zimbabwe

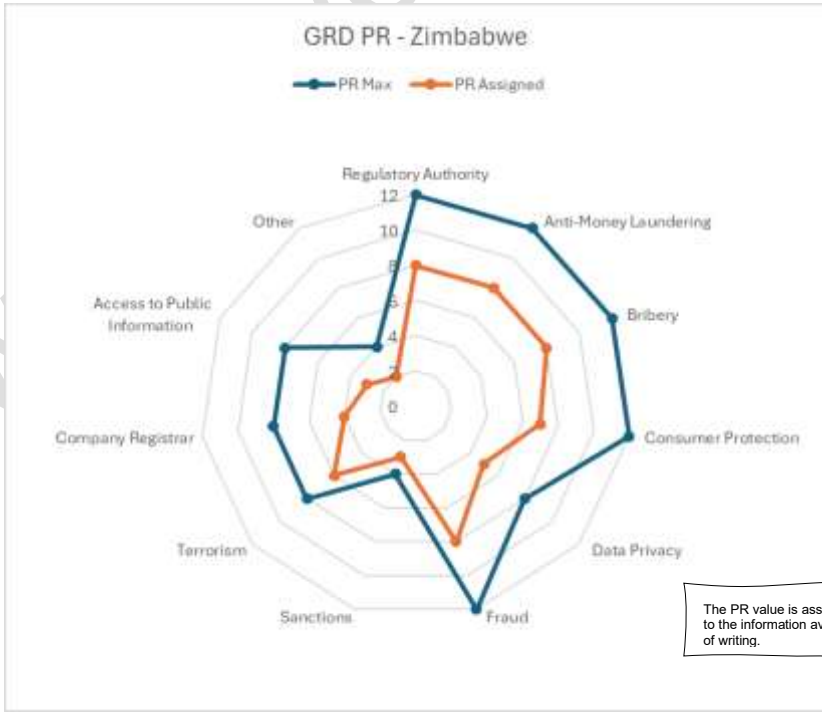
The PR value of **6.3** is derived using the following assigned values:

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other
PR Max	12	12	12	12	8	12	4	8	8	8	4
PR Assigned	8	8	8	7	5	8	3	6	4	3	2

Zimbabwe has defined several regulations and laws which are supported by miscellaneous processes to support the domains and any international obligations.

There are many strengths within Zimbabwe's domains; however, the multi-currency system and the lack of digital channels are reflected in the value assigned for posture.

NB**: The figure does not reflect the execution of processes, laws and regulations.**



Consolidated Posture Ratings Table (2025)

Below is a consolidation of all Posture Ratings assigned in this book. The Table is valid at the time of writing (May 12th 2025).

	Regulatory Authority	Anti-Money Laundering	Bribery	Consumer Protection	Data Privacy	Fraud	Sanctions	Terrorism	Company Registrar	Access to Public Information	Other	GRD-PR
Maximum Ceiling Value ->	12	12	12	12	8	12	4	8	8	8	4	
Argentina	10	6	6	4	7	6	3	6	6	6	3	**6.3**
Armenia	9	8	5	6	4	6	2	5	6	4	2	**5.7**
Australia	9	10	9	9	6	9	3	7	6	7	2	**7.7**
Austria	10	9	7	6	6	8	3	5	8	4	2	**6.8**
Bahrain	10	9	7	9	5	8	2	5	6	3	2	**6.6**
Bangladesh	9	9	8	9	3	7	3	5	7	6	3	**6.9**
Belgium	9	9	7	7	6	8	3	6	6	7	2	**7**
Bermuda	9	9	8	7	7	8	3	5	6	6	2	**7**
Brazil	8	9	5	8	6	5	2	4	5	4	2	**5.8**
Brunei Darussalam	8	8	6	6	4	6	3	5	5	4	2	**5.7**
Bulgaria	7	7	6	6	4	7	2	4	4	6	2	**5.5**
Canada	9	8	8	7	6	8	3	6	6	7	3	**7.1**
Chile	8	8	7	8	3	6	2	5	5	4	2	**5.8**
China (SAR) – Macau	8	7	6	6	6	7	2	5	3	0	2	**5.2**
Croatia	7	7	8	8	6	7	2	5	4	3	2	**5.9**
Cyprus	7	7	7	8	6	7	2	5	4	4	2	**5.9**
Czech Republic	7	8	7	9	5	8	2	5	5	5	2	**6.3**
Denmark	9	8	8	8	6	8	3	5	6	5	2	**6.8**
Egypt	8	8	7	6	5	6	2	5	4	5	2	**5.8**
Estonia	8	7	7	6	5	7	2	5	4	5	2	**5.8**
Federal Republic of Nigeria	7	7	7	6	5	6	2	6	6	6	2	**6**
Finland	9	8	9	7	6	8	2	5	5	4	3	**6.6**
France	9	8	8	8	6	8	2	6	6	7	2	**7**
Germany	10	8	8	8	6	8	3	6	6	5	2	**7**
Greece - The Hellenic Republic	9	7	9	7	6	8	3	6	5	5	2	**6.7**
Hashemite Kingdom of Jordan	8	7	8	6	5	6	2	5	6	7	2	**6.2**
Hong Kong	9	9	9	7	6	8	2	6	7	7	2	**7.2**
Hungary	9	7	8	8	5	8	2	5	6	6	3	**6.7**
India	8	8	7	7	5	8	2	5	5	6	2	**6.3**
Indonesia	8	8	6	6	6	7	2	5	5	4	2	**5.9**
Iran	7	4	5	5			1	3		2	2	**2.9**
Ireland (Republic of)	9	8	8	7	6	8	2	6	6	5	3	**6.8**
Isle of Man	7	8	8	8	6	8	2	6	6	6	2	**6.7**
Israel	8	8	7	7	6	9	3	6	6	6	2	**6.8**
Italy	9	8	8	9	6	8	3	6	6	5	2	**7**
Japan	10	9	9	10	7	10	3	6	6	5	3	**7.8**
Jersey	7	7	8	8	7	9	3	6	7	6	2	**7**
Republic of Kenya	9	8	8	6	7	7	3	5	6	6	2	**6.7**
Latvia	8	7	8	7	5	6	3	5	6	4	2	**6.1**
Lebanon	7	6	5	5	3	4	2	3	5	3	2	**4.5**
Luxembourg	10	9	7	8	6	7	3	5	6	7	3	**7.1**
Malaysia	9	9	9	8	7	8	2	4	6	2	2	**6.6**
Mauritius	9	9	8	7	6	8	3	5	5	6	2	**6.8**
Mexico - United Mexican States	9	8	7	8	7	8	3	5	3	6	2	**6.6**
Netherlands	9	8	7	8	6	8	3	6	6	6	3	**7**
New Zealand	9	9	8	9	7	8	2	5	6	7	2	**7.2**
Peoples Republic of China	9	9	9	8	5	9	2	6	5	6	2	**7**
Qatar	8	7	7	6	5	7	3	5	5	5	2	**6**
Republic of Lithuania	9	9	8	7	5	7	2	6	5	6	2	**6.6**
Russia	9	9	8	6	5	8	2	5	5	5	3	**6.5**
Saudi Arabia	9	8	8	8	5	8	3	5	5	6	3	**6.8**
Singapore	8	8	8	7	6	8	2	6	6	7	2	**6.8**
South Africa	8	8	9	7	5	8	3	5	5	5	2	**6.5**
South Korea	8	8	8	9	7	9	2	6	6	7	2	**7.2**
Switzerland	9	9	9	7	6	7	3	6	7	7	2	**7.2**
Thailand	8	7	4	2	3	4	3	4	6	4	1	**4.6**
The Sultanate of Oman	6	8	4	6	6	6	2	5	5	5	3	**5.6**
Türkiye	9	7	6	8	5	6	2	5	7	5	2	**6.2**
UK	11	9	9	8	6	9	3	7	7	7	2	**7.8**
United Arab Emirates (UAE)	9	8	8	7	5	7	2	6	5	6	3	**6.6**
USA	11	10	11	10	6	10	3	7	7	7	3	**8.5**
Vietnam	7	5	6	6	5	6	3	5	5	5	2	**5.5**
Zimbabwe	8	8	8	7	5	9	3	6	4	3	2	**6.3**

Valid as of 3rd May 2025

MISCELLANEOUS INFORMATION

Recommended Global Sources of additional Information.

The following are sources of generic information relating to specific domains and are provided as links we recommend visiting.

	Source / Description
Central Banking	https://www.bis.org/ (i) https://www.bis.org/reshub/whatsnew.htm?m=62 (ii) https://www.eccb-centralbank.org (iii) https://www.ndb.int/ (iv) https://www.ecb.europa.eu/paym/target/target2/html/index.en.html (v)

The Bank for International Settlements (**BIS**) mission is to support the central banks' pursuit of monetary and financial stability through international cooperation and to act as a **bank for central banks.**

(i)

BIS publish numerous documents through the Research Hub.

(ii)

The Eastern Caribbean Central Bank (**ECCB**) was established in October 1983. It is the Monetary Authority for a group of eight island economies namely - Anguilla, Antigua and Barbuda, Commonwealth of Dominica, Grenada, Montserrat, Saint Christopher (St Kitts) and Nevis, Saint Lucia and Saint Vincent and the Grenadines.

(iii)

The New Development Bank (**NDB**) is a multilateral development bank established by Brazil, Russia, India, China and South Africa (**BRICS**) with the purpose of mobilizing resources for infrastructure and sustainable development projects in emerging markets and developing countries (**EMDCs**).

(iv)

TARGET2 is the real-time gross settlement (**RTGS**) system owned and operated by the Eurosystem. Central banks and commercial banks can submit payment orders in the euro to TARGET2, where they are processed and settled in central bank money, i.e. money held in an account with a central bank.

(v)

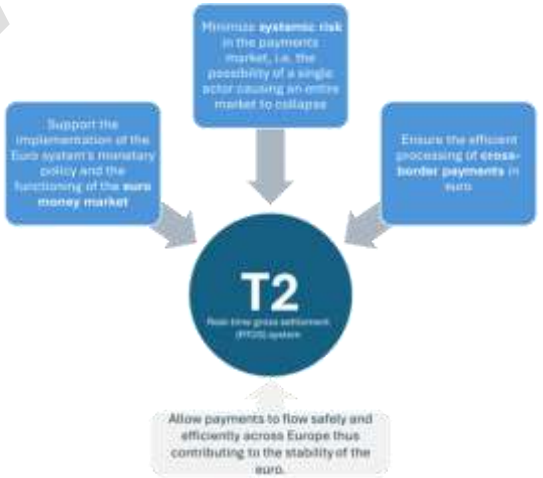
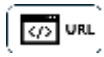
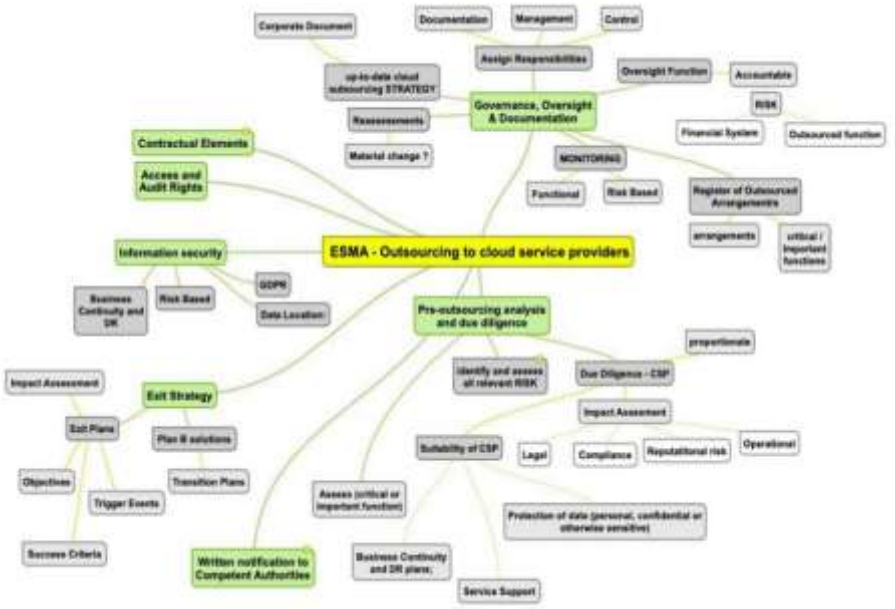


Figure 40 EU T2 Real-time gross settlement (RTGS) system

	Source / Description
AI	https://oecd.ai/en/ (i) https://artificialintelligenceact.eu/ (ii) https://au.int/en/documents/20240809/continental-artificial-intelligence-strategy (iii) The **Organization** for **E**conomic **C**o-operation and **D**evelopment (**OECD**) is an international organization that works to build improved policies for better quality. The OECD provides AI tools, data and other AI policy resources that are accessible for developed and developing countries. (i) In 2021, the European Commission implemented the world's first comprehensive AI law, the **EU AI Act**. The Act groups AI applications and systems into three risk categories and outlines how to regulate each accordingly. (ii) Many African countries are Member States of the African Union (AU). Whilst many of these countries do not have standalone AI policies/strategies, many AU Member States follow the recommendations outlined in the **Continental Artificial Intelligence Strategy of 2024.** (iii)
Fraud	https://anti-fraud.ec.europa.eu/system/files/2023-07/pif-report-2022-325-tfeu_en.pdf The EU Working Document referencing the measures adopted by the EU Member States to protect the EU's financial interests with the implementation of article **325 TFEU.** The 34th Annual Report on the protection of the European Union's financial interests and the fight against fraud - 2022.
Anti- Money Laundering and Financing of Terrorism	https://eurasiangroup.org/en (i) https://www.gafilat.org/index.php/es (ii) The **Eurasian Group** (EAG) on combating Money Laundering and the financing of terrorism is an FATF-style regional body established in 2004. The primary goal of the EAG is to ensure effective interaction and cooperation at regional levels. The EAG promotes the integration of member-states into the international system of anti-money laundering and combating financing of terrorism in accordance with the recommendations of the FATF. (i) The FATF of Latin America (**GAFILAT**) is a regionally based intergovernmental organization that brings together 18 countries in South, Central America and North America. GAFILAT was created to prevent and combat money laundering, terrorist financing and the financing of the proliferation of weapons of mass destruction. (ii)

	Source / Description
Sanctions	 https://www.un.org/securitycouncil/sanctions/information (i) https://www.afdb.org/en/projects-operations/debarment-and-sanctions-procedures (ii) https://lnadbg4.adb.org/oga0009p.nsf (iii) https://www.iadb.org/en/who-we-are/transparency/sanctions-system/sanctioned-firms-and-individuals (iv) **The United Nations Security Council** can take action to maintain or restore international peace and security under Chapter VII of the UN Charter. Sanctions measures, under Article 41, encompass a broad range of enforcement options that do not involve the use of armed force – see www.kyc-data.com. (i) **The African Development Bank Group** maintains a list of sanctioned individuals and firms, alongside those that have been sanctioned by signatories to the Agreement for Mutual Enforcement of Debarment Decisions. Sanctions are imposed on entities found to have participated in coercive, collusive, corrupt, fraudulent or obstructive practices under the Bank's sanctions system or adopted under the Agreement for Mutual Enforcement of Debarment Decisions. (ii) **Asian Development Bank** has a published sanctions list which contains the names of entities who violated the sanctions while ineligible, entities who committed second and subsequent violations, debarred entities who are uncontactable and cross-debarred entities. (iii) **Inter-American Development Bank**. (IDB) firms and individuals listed who have been sanctioned for having engaged in fraudulent, corrupt, collusive, coercive or obstructive practices (collectively, prohibited practices), in violation of the IDB group's sanctions procedures and anti-corruption policies. (iv)
EU Directive AML & Terrorist Financing.	 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L0849&from=EN DIRECTIVE (EU) 2015/849 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (20 May 2015). The prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) **No 648/2012** of the European Parliament and of the Council.
Cloud Adoption Policy – EU SMA	 https://www.eba.europa.eu/sites/default/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf The European Banking Authority Guidelines on outsourcing arrangements issued 25 February 2019 (**EBA Guidelines**). The EBA Guidelines apply to EU-regulated credit institutions, investment firms, electronic money institutions and payment institutions and provide guidance to these entities when they are using or planning to use cloud services.

	Source / Description
	URL https://www.esma.europa.eu/sites/default/files/library/esma_cloud_guidelines.pdf ESMA Guidelines on Outsourcing to Cloud Service Providers. Below is a simple mind map that highlights the key areas found in the document. 
Technology	https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en The Digital Operational Resilience Act (**DORA**) is an EU regulation that came into force on the 17th of January 2025. It aims to strengthen the IT security of financial entities such as banks, insurance companies and investment firms and making sure that the financial sector in Europe can stay resilient in the event of a severe operational disruption. DORA standardizes the rules relating to operational resilience for the financial sector applying to 20 different types of financial entities and ICT third-party service providers.
Misc	https://www.weforum.org/publications/the-global-competitiveness-report-2020/ (i) https://cacj-ajp.org/ (ii) Global Competitiveness Report Special Edition 2020: How Countries are Performing on the Road to Recovery. (i) The ASEAN Judiciaries Portal (**AJP**) the website for the Council of ASEAN Chief Justices (**CACJ**) formerly known as the ASEAN Chief Justices Meeting (**ACJM**) established in Singapore on 23 August 2013. (ii)

Global Currency Data – Not Available in free edition

In the table below we present a list of currencies with their ISO code and comments relating to the notes in circulation at the time of writing.

Posture Rating (PR)

The GRD Posture Rating (PR) is a **notional value** which provides a cursory indicator of the regulatory posture. At a minimum, it encapsulates three variables; the availability of information, tools that support compliance and processes available to support the desired domain outcomes.

The *PR value is **not an indicator or measure of risk*** **and** in essence, no direct correlation exists between Posture and risk, but it is worthy of mention for clarity.

Risk is assessed based on the probability of a disruptive event impacting either service delivery or business operations, reflecting uncertainty regarding the effects or implications of an activity.

Risk Assessment involves the identification of **threats, *vulnerabilities*** and any ***consequences*** which subsequently inform the development of controls and strategies to mitigate any possible risks.

Figure 41 Risk attributes

A risk can have a direct relationship to a threat or vulnerability meaning any mitigation or control can eliminate the risk. Hence, risks are binary, i.e. they either exist or they do not, which cannot be said for posture.

Posture is a term used to represent the overall *position and standing* of the human body in relation to the environment and space it occupies especially while standing, sitting, or lying down and how balance and symmetry is maintained during dynamic movements.

A good posture reflects equilibrium in relation to movement and general good health.

Domains are areas of regulatory concentration in which the Government of a country has a duty of care, to control and manage on behalf of its citizens whilst meeting any international obligations. Domains can be assessed through multiple lenses, which when combined provide a holistic view of a country's ability to deliver quality services whilst protecting potential inbound investment.

PR - Posture Ratings are notional values which represent the sum of all values assigned to the domains of a country, they act as an indicator of traits and capabilities in relation to domains for a country.

Figure 42 -PR Score Considerations.

Scores are assigned at the discretion of an analyst. The analyst is responsible for reviewing domain data and creating context from the material available in the public domain for the GRD. At a minimum, the scores will consider the following in three categories Support, Tools and Processes as depicted below, where;

- Support
  - Help Desk – Is there a central point of contact or channel for event reporting, complaint logging and assistance requests within this domain?
  - Publications – Domain information is freely available from the central domain websites or delegated regulatory authorities.
  - Guidance - The level of information provided to ensure firms or individuals are compliant with detailed process maps and other visuals to simplify the understanding of the domain compliance framework.
  - Usability of the service for the above.
- Tools
  - Availability of tools that support domain understanding or delivery i.e. any bespoke tools that make the job of compliance for the domain smoother.
  - Digital Channels such as domain websites, mobile apps, kiosks etc.
  - Usability of the services refers to the accessibility and ease of use of any screen flows, particularly for the general population, including individuals with visual impairments.
- Process
  - Laws and any legally binding rules that govern interactions between citizens and the state and are used to enforce any actions set out in policies and can be enforced by courts.
  - Regulations are usually created by an executive branch of a government and are the rules that provide instructions for how to enforce laws.
  - Policies i.e. the *principles* and *guidance* that outline expected behaviours and goals.
  - Institutions that support the domain are seen as a major indicator of the commitment – NB any absence of institutions for a domain will result in a poor score.
  - Digital Channels for any or all the above is crucial for delivering the regulatory processes and weighted accordingly.

While we appreciate there is no single, reusable formula or patterns for scoring a regulatory domain, the above provides a set of guiding principles to support the allocation of a notional score. This score offers an indicative assessment, rather than a definitive one.

Not all domains are equal in importance and as such are weighted according to the domains to reflect the perceived value for the system. Please note the Sanctions Regime is weighted low because most countries leverage the UN Sanctions list as default.

The weighting in total is 100 and each domain is allocated a value which provides a percentage value which is represented in the www.kyc-data.com portal.

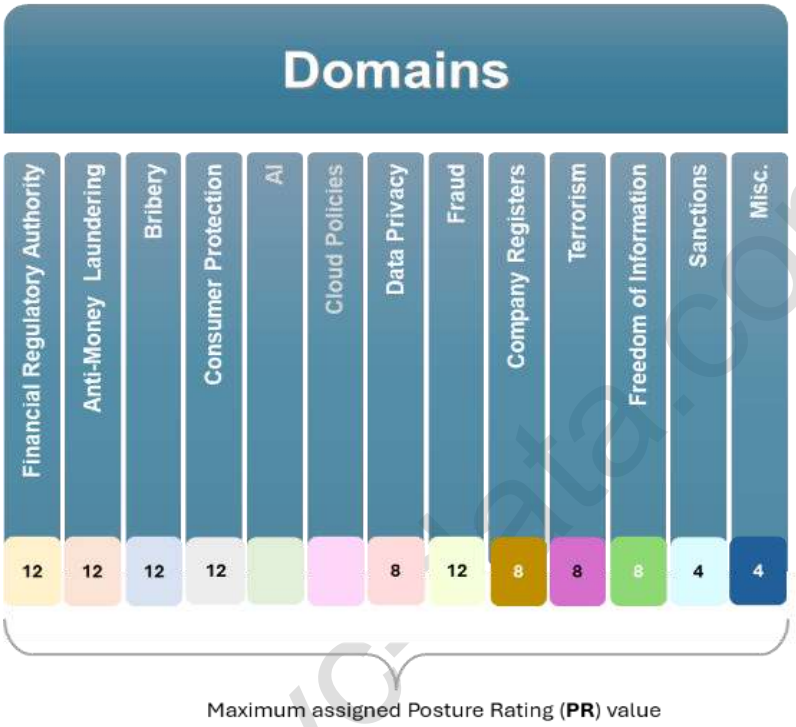


Figure 43 Domain Weightings

Glossary of Terms / Acronyms

The following table lists some of terms and acronyms used throughout this book which may not have been detailed.

Acronym	Name	Description
CDD	Customer Due Diligence	The process by which financial institutions identify and verify the identity of their clients, monitor transactions and report suspicious activity to the regulator.
ECOWAS	Economic Community of West African States - https://www.ecowas.int/	The Economic Community of West African States is a regional political and economic union of fifteen countries located in West Africa. ECOWAS can impose Sanctions on behalf of its members.
FATF	The Financial Action Task Force	The Financial Action Task Force (FATF) leads global action to combat money laundering, terrorist and proliferation financing. The FATF conducts research into how money is laundered, terrorism is funded and promotes global standards to mitigate the risks with the assessment of how countries are taking effective action. FATF country assessments are prepared with the assistance of the World Bank and the International Monetary Fund to evaluate compliance with the standards – including in non-member countries.
PR	Posture Rating	The PR is a **notional indicative value** between the range of 1 and 10 that reflects the information and countries processes available to support the domains. The PR is **not a risk rating** and should not be used as such. For each domain the following weighting has been assigned;  A value is designated by our analyst to each domain based on the availability of the information, process and public tools to enable the desired outcomes for the domains. The PR value published in the GRD is current at the time of writing, however, a more accurate figure is maintained and updated regularly at the www.kyc-data.com portal.
URL	Uniform Resource Locator	A URL is an address of a given unique resource on the Web. A valid URL points to a unique resource. Such resources can include a webpage, file or document.
VPN	Virtual Private Network	A VPN establishes a digital connection between a computer and a remote server owned by a VPN provider, creating **a point-to-point tunnel** allowing for the encryption of data, masking the IP address and the bypass of possible firewalls via the internet. Many countries, either directly or indirectly, seek to limit and control the data and content flow via a VPN leaving or entering the country.