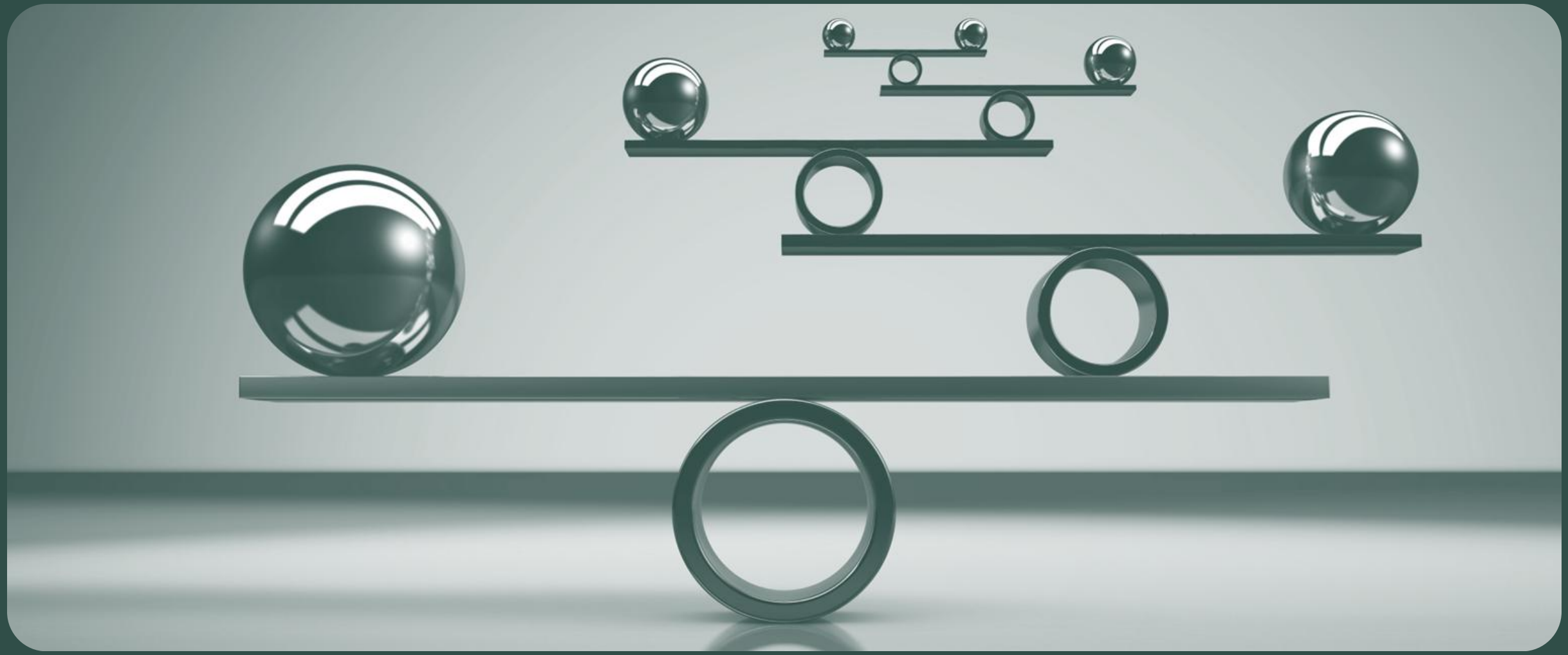
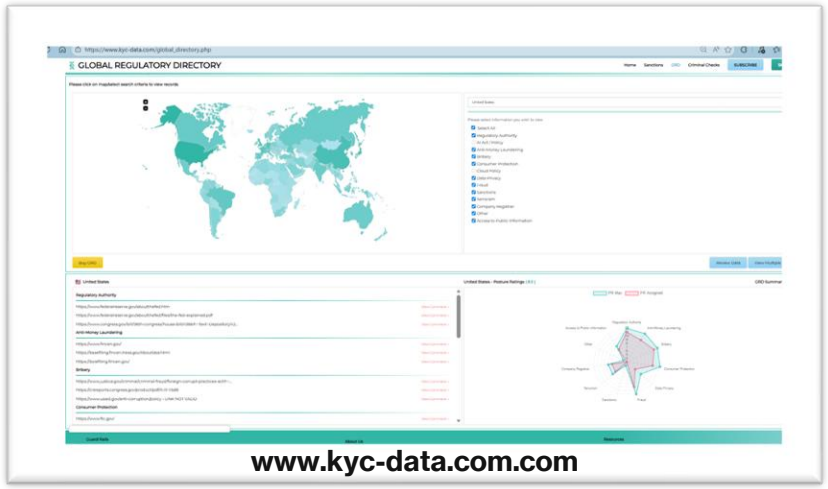


Appreciating Global Regulatory Requirements when Developing The Enterprise Systems Blueprint

Wednesday 4th February 2025

Daljit R Banger

Agenda



www.kyc-data.com.com

The Why

- Open Question
- User Story
- Example Fines
- Drivers for Change

Regulatory Domains

- Understanding the Impact for Regulatory Compliance on the Enterprise Ecosystem
  - System
  - Business

Summary

- Regulatory Compliance – Impact on the Enterprise Technology Ecosystem
- Q&A

Does your organisation .....

DELIVER SERVICES IN OR FOR A REGULATED INDUSTRY

OPERATE ACROSS MULTI JURISDICTIONS

PROCESS OR STORE PERSONAL DATA

USE REGIONALLY CLOUD BASED SERVICES

SELL CONSUMER GOODS

PROVIDE ADVISORY TO GOVERNMENT

YES

MAYBE

If you have answered either *Yes* or *Maybe* to one or more of the questions, then your will need to understand your Regulatory obligations to deliver the Enterprise Architecture Blueprints

As a user, I need to know my systems and processes are compliant with any regulatory obligations my enterprise is subject to.

Organisations operating across multiple jurisdictions need to be cognisant of the impact from global and regional regulatory authorities and must minimise the possible ramifications of noncompliance.

Controls should be designed and where possible ‘built into’ enter Enterprise Systems to address any risks. Its s important for the Architecture Community and those who design enterprise capabilities and systems to be conversant with the regulatory requirements The organization is exposed to.

Failure to observe or comply with these requirements can result in financial penalties.

Example Fines

Nov 2025 : **UK's** FCA fines Nationwide **£44m** for failings in financial crime controls

Dec 2024 : **Hong Kong** Monetary Authority imposed a pecuniary penalty of **HK$4,000,000** against China CITIC Bank International Limited (CITIC)

Oct 2024 : **US** FinCEN assessed a record **$1.3 billion** penalty against TD Bank

Oct 2020 :The Federal Court of **Australia** has today ordered Westpac to pay a **$1.3** billion

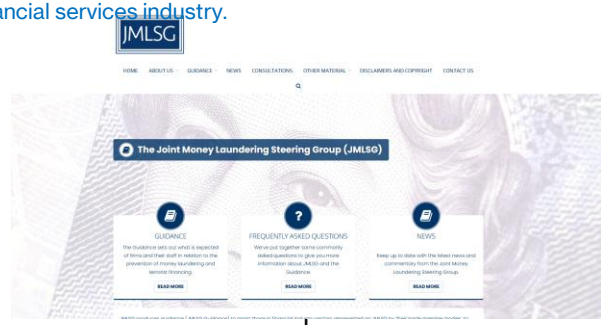
2017 : Central Bank of **Paraguay** imposed a **USD 9.6 million** fine on **Brazil's** Banco

Sept 2024 : **South African** Reserve Bank fines the Old Mutual Life Assurance Company (South Africa) Limited **R15.9 million**

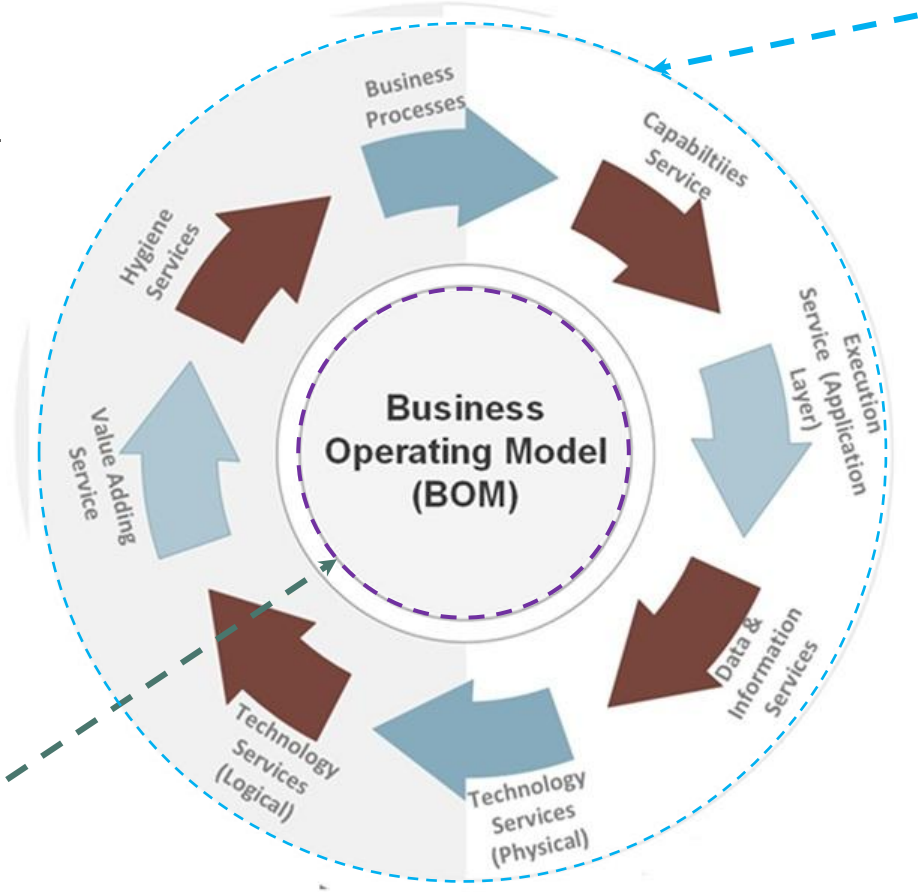
Oct 2024 :The Financial Intelligence Unit (FIU) fined the Union Bank of **India Rs 5.4** Million

The Guidance is issued by a private sector body and therefore cannot be legally binding, although it is of significance that it **has HM Treasury approval.** It is **not over-prescriptive** but provides a **base** from which management can develop tailored **policies and procedures** that are appropriate for their business. It remains the responsibility of a firm to make its own judgment on individual cases, on a **risk-based approach**.

The Joint Money Laundering Steering Group (JMLSG) is a private sector body that is made up of the leading UK Trade Associations in the financial services industry.



Core
(Business Specific)



Operational
(System Specific)

EU
Digital Operational Resilience Act (DORA)

ICT Risk Management
- Article 5 Governance & Organisation
- Article 6 - ICT Risk Management Framework
- Article 7 – Systems , Protocols & Tools
- Article 8 - Identification
- Article 9 – Protection and Prevention
- Article 10 - Detections
- Article 11 – Response & Recovery
- Article 12- Backup (policies & procedures)
- Article 13 – Learning & evolving
- Article 14 Communication
- Article 15 – Harmonisation
- Article 16 Simplified ICT Risk mgmt. framework

ICT Incident management, classification and reporting
- Article 17 – ICT Incident mgmt. Process
- Article 18 – Classification
- Article 19 – reporting
- Article 20 – Harmonisations
- Article 21 – centralisation of reporting ICT incidents
- Article 22 _ Supervisory feedback
- Article 23 – Operational / security related payment incidentS

Digital Operational Reliance Testing
- Article 24 – General
- Article 25 Testing of ICT tools and systems
- Article 26 – Advanced tools – Threat-Led Penetration Testing (TLPT)
- Article 27 – requirements for Testers carrying out TLTP

Managing of ICT 3rd part risk
- Article 28 – General
- Article 28 – Assessment of risk at entry level
- Article 30 – Key contractual provisions

Oversight Framework of critical ICT third-party service providers
- Article 31 - Designation of critical ICT third-party service providers
- Article 32 - Structure of the Oversight Framework
- Article 33 - Tasks of the Lead Overseer
- Article 34 -Operational coordination between Lead Overseers
- Article 35 - Powers of the Lead Overseer
- Article 36 -Exercise of the powers of the Lead Overseer outside the Union
- Article 37 - Request for information
- Article 38 - General investigations
- Article 39 - Inspections
- Article 40 -Ongoing oversight
- Article 41 - Harmonisation of conditions enabling the conduct of the oversight activities
- Article 42 - Follow-up by competent authorities
- Article 43 - Oversight fees
- Article 44 - International cooperation

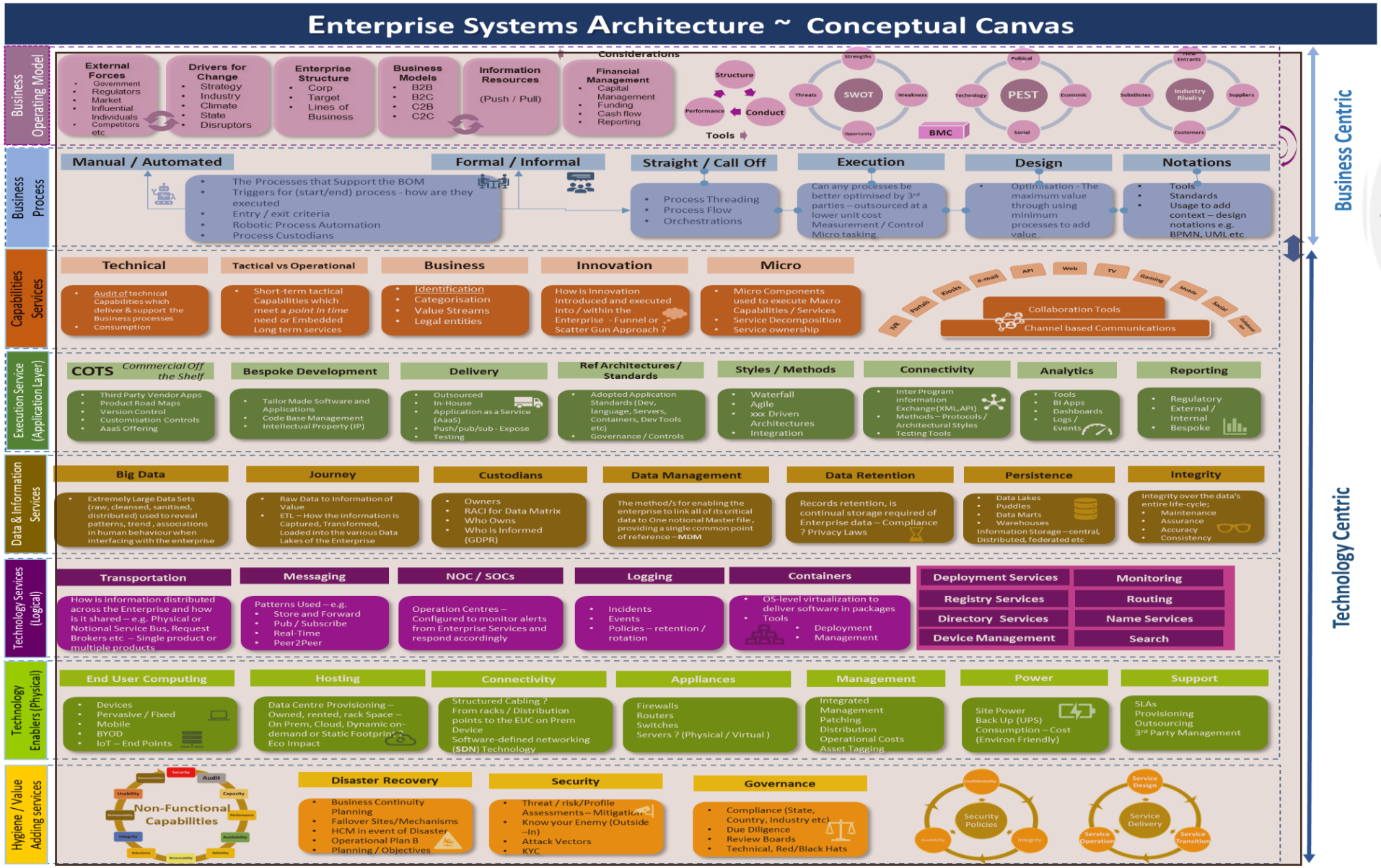
Information-sharing arrangements
- Article 45 - Information-sharing arrangements on cyber threat information and intelligence

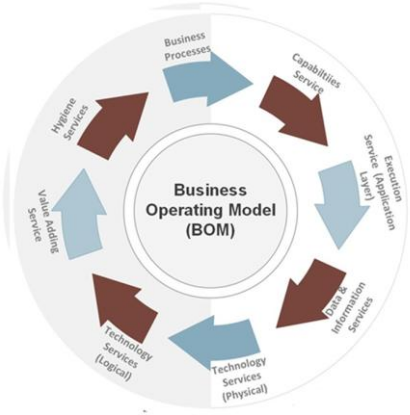
Competent authorities
- Article 46 - Competent authorities
- Article 47 - Cooperation with structures and authorities established by Directive (EU) 2022/2555
- Article 48 - Cooperation between authorities
- Article 49 - Financial cross-sector exercises, communication and cooperation
- Article 50 - Administrative penalties and remedial measures
- Article 51 - Exercise of the power to impose administrative penalties and remedial measures
- Article 52 - Criminal penalties
- Article 53 - Notification duties
- Article 54 - Publication of administrative penalties
- Article 55 - Professional secrecy
- Article 56 - Data Protection

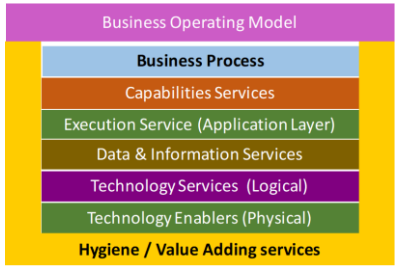
Delegated acts
- Article 57 - Exercise of the delegation

Transitional and final provisions
- Articles - 58 onwards - Misc

Understanding the Impact for Regulatory Compliance on the Enterprise Ecosystem







System Specific Regulations

- Cloud Hosting Policies
- Data Privacy / Residency
- Emerging AI Acts / Policies

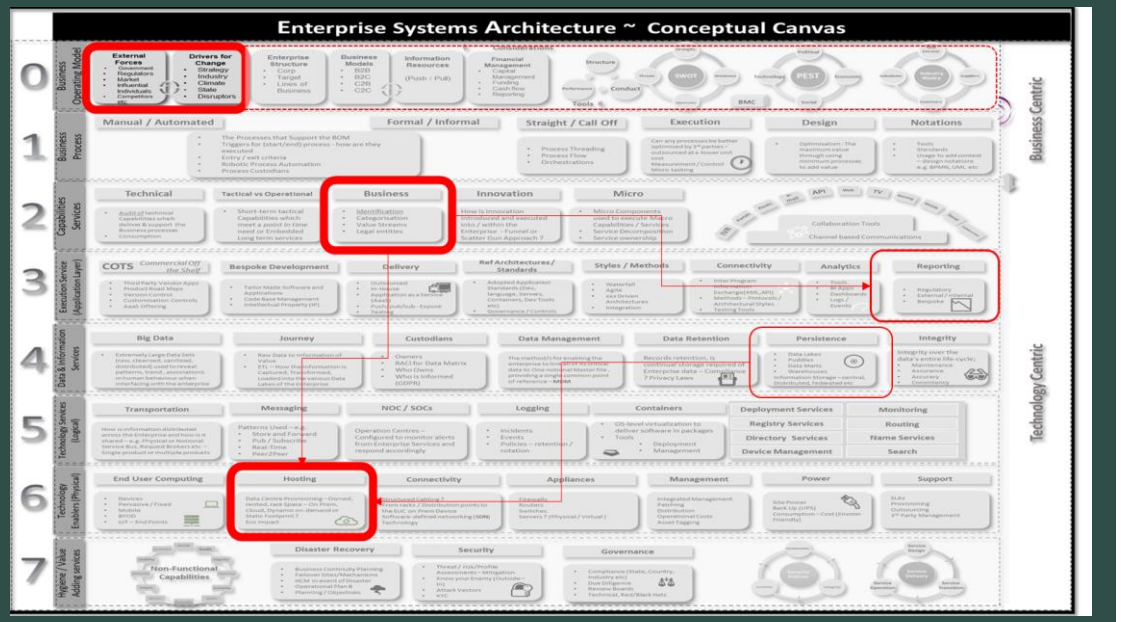
System Specific Regulations

Cloud hosting Policies | **Data Privacy** | **AI Act / 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.



Example

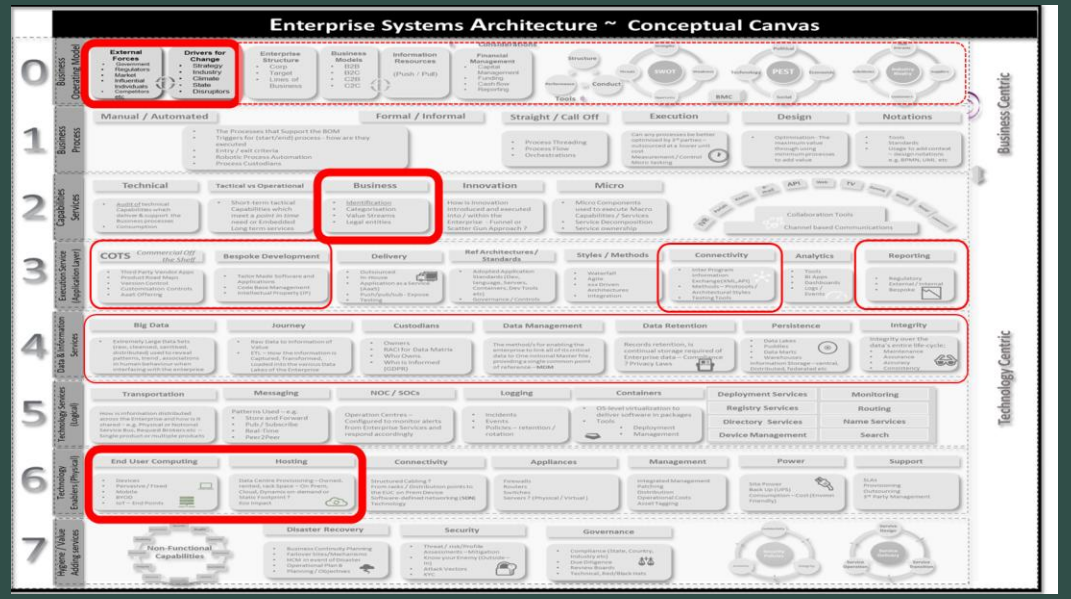
Mexico's **National Digital Strategy** aims to achieve the goal of a *'Digital Mexico'* through the adoption of Information Communication Technologies (ICTs) to maximise economic, social and political impact. The **National Digital Strategy Coordination Office of the President's Office** is responsible 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.

System Specific Regulations

Cloud hosting Policies | **Data Privacy** | AI Act / Policy

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.



Example

The Personal Information Protection Commission (**PPC**)
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.
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**

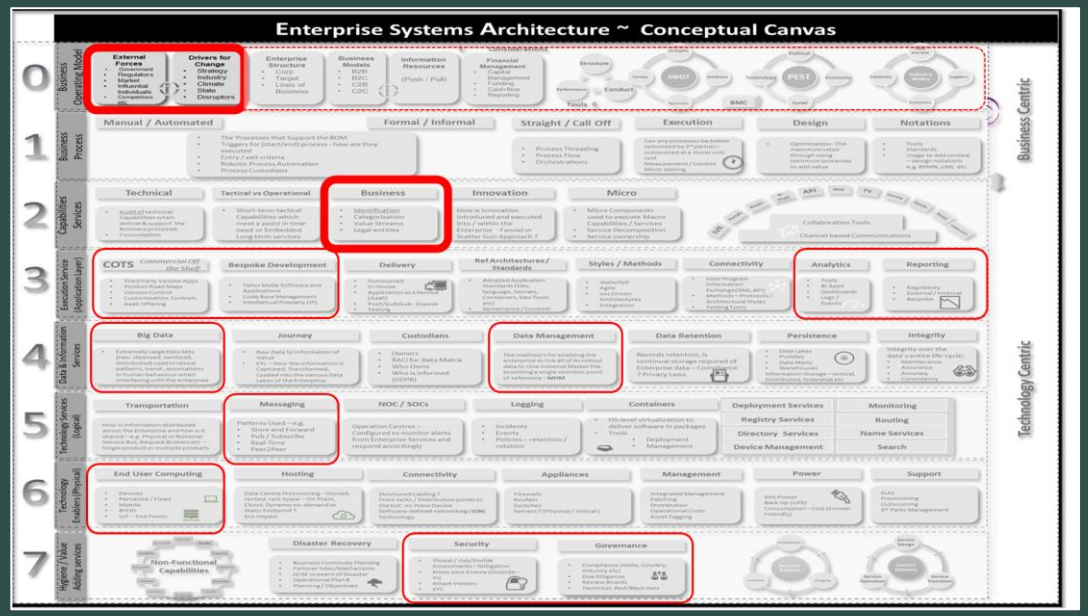
System Specific Regulations

Cloud hosting Policies | Data Privacy | AI Act / Policy

Artificial Intelligence (AI) refers to a set of technologies that enable Information Systems to perform cognitive functions usually associated with humans.

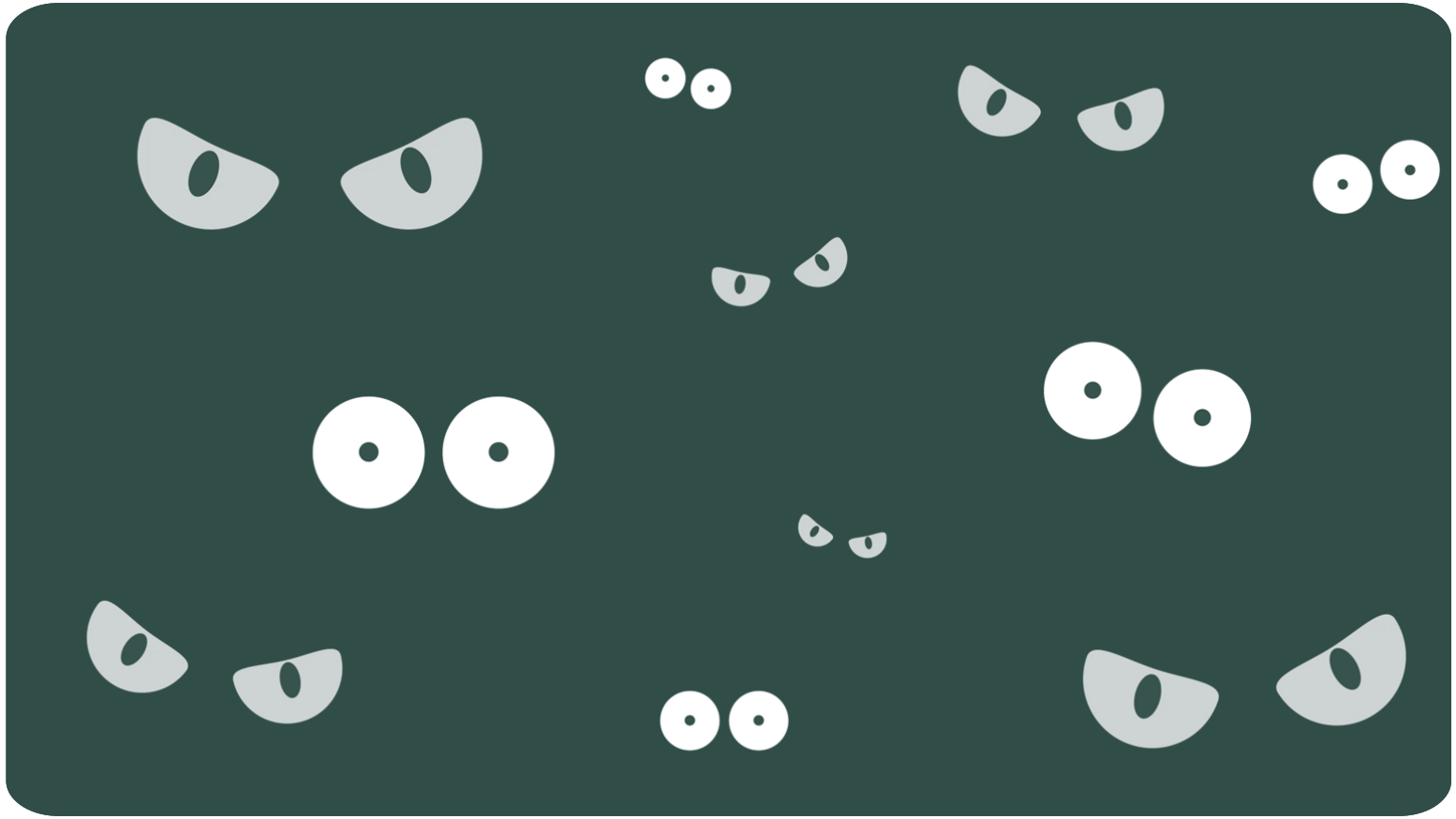
AI systems based on machine learning (ML), with the increasing sophistication of generative AI, produce various types of content, including *text, imagery, audio and synthetic data* all of which can impact elements of **privacy** and intellectual property(**IP**).

Governments are introducing legislation and policies to support the control and introduction of AI into society.



Business Specific

- Bribery
- Consumer Protection
- Anti-Money Laundering
- Fraud
- Sanctions
- Terrorism

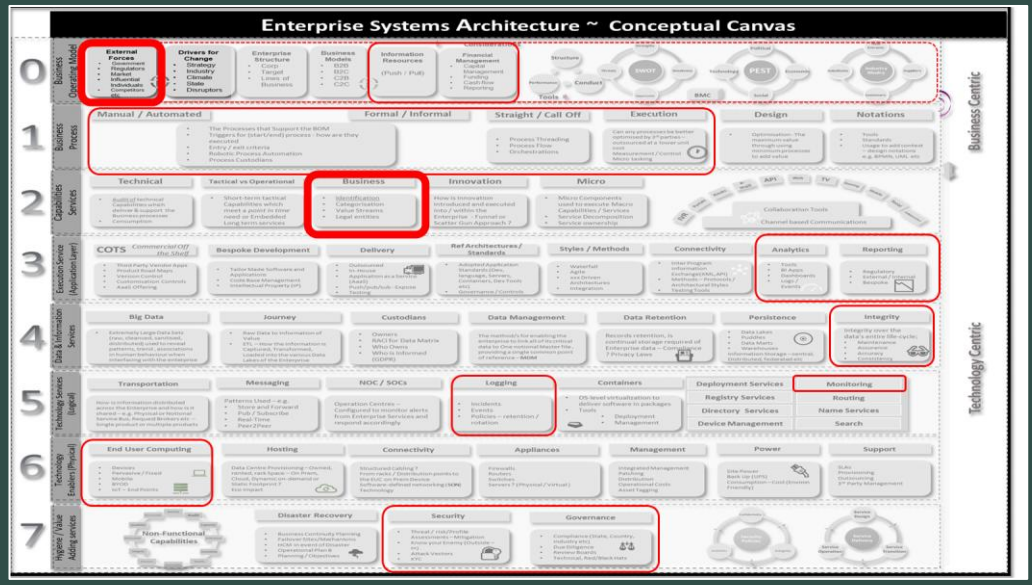


Business Specific

Bribery | **Consumer Protection** | **Anti-Money Laundering** | **Fraud** | **Sanctions** | **Terrorism**

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 unique laws,** policies and practices to prevent bribery.



Example

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)

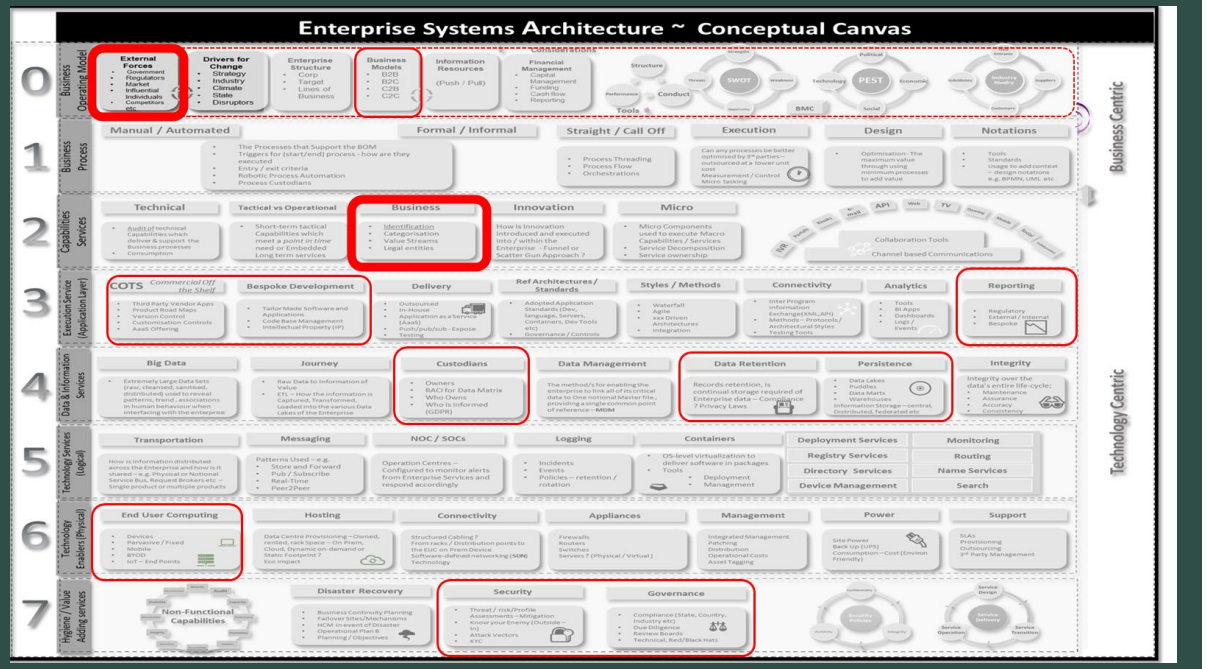
The Malaysian Anti-Corruption Commission (MACC) is an independent regulatory body, authorised by the Anti-Corruption Commission Act 2009 to investigate and prevent any form of corruption and abuse of power in Malaysia. Their main functions are as follows:
1. Receiving and handling reports/complaints 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)

Business Specific

Bribery | **Consumer Protection** | Anti-Money Laundering | Fraud | Sanctions | Terrorism

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



Example

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:

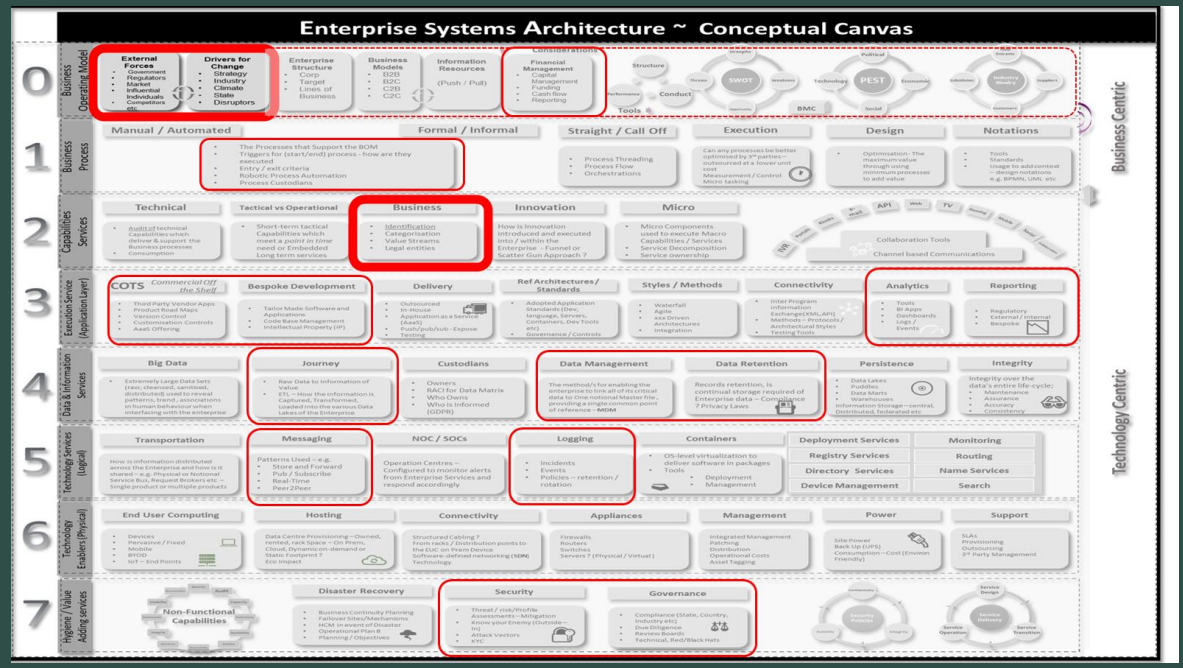
1. Problems with product or services - **Consumer Guarantees Act**
2. Problems with borrowing money or using credit - **Credit Contracts and Consumer Finance Act**
3. Businesses acting in a misleading or unfair way – **Fair Trading Act**
4. Protection of personal information – **Privacy Act**

Business Specific

Bribery | Consumer Protection | Anti-Money Laundering | Fraud | Sanctions | Terrorism

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.



Example

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:

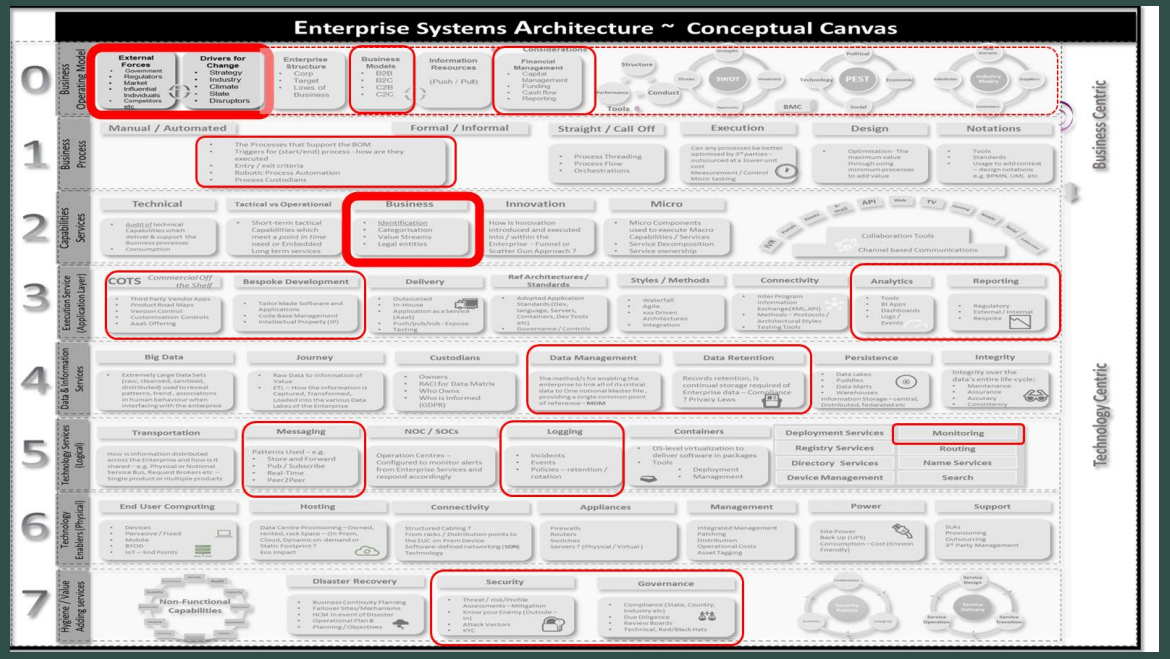
- Promoting **transparency** of associations with high levels of terrorist financing risk
- Updating of client data and **suspicious activity** reports relating to money laundering

Business Specific

Bribery | Consumer Protection | Anti-Money Laundering | **Fraud** | Sanctions | Terrorism

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. .



Example

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.

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**

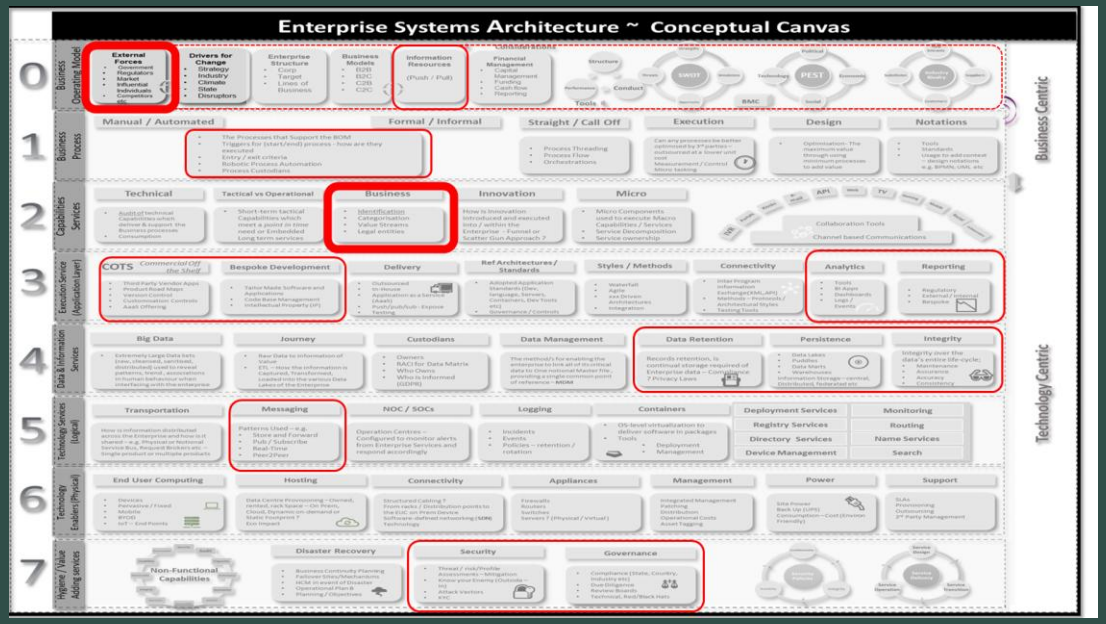
Business Specific

Bribery | Consumer Protection | Anti-Money Laundering | Fraud | **Sanctions** | Terrorism

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**



Example

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 **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.

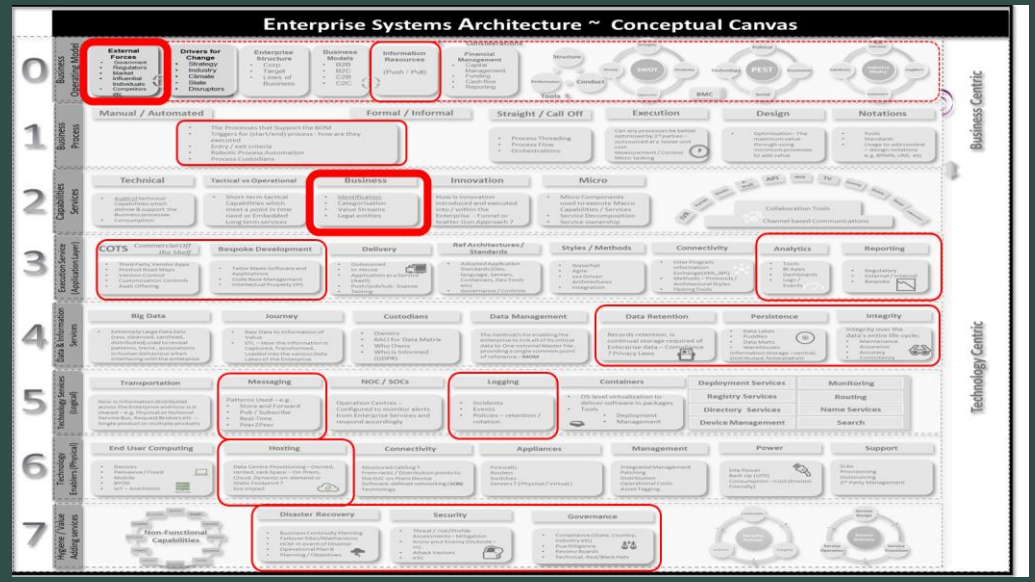
Business Specific

Bribery | Consumer Protection | Anti-Money Laundering | Fraud | Sanctions | **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:

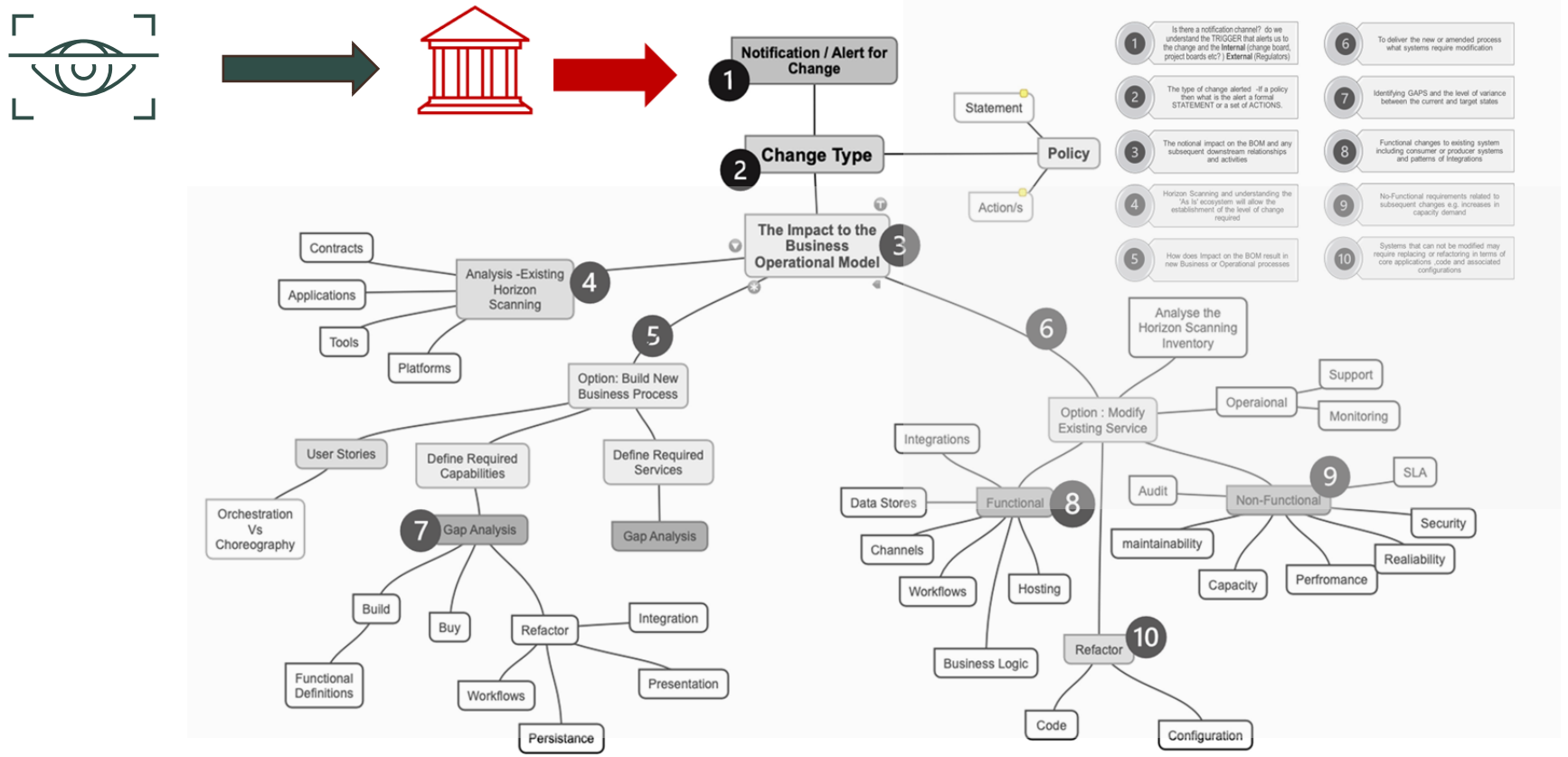
- Those who commit or participate in acts of terrorism.
- Those who prepare for acts of terrorism.
- Those who promote or encourage terrorism (including the unlawful glorification).



Example

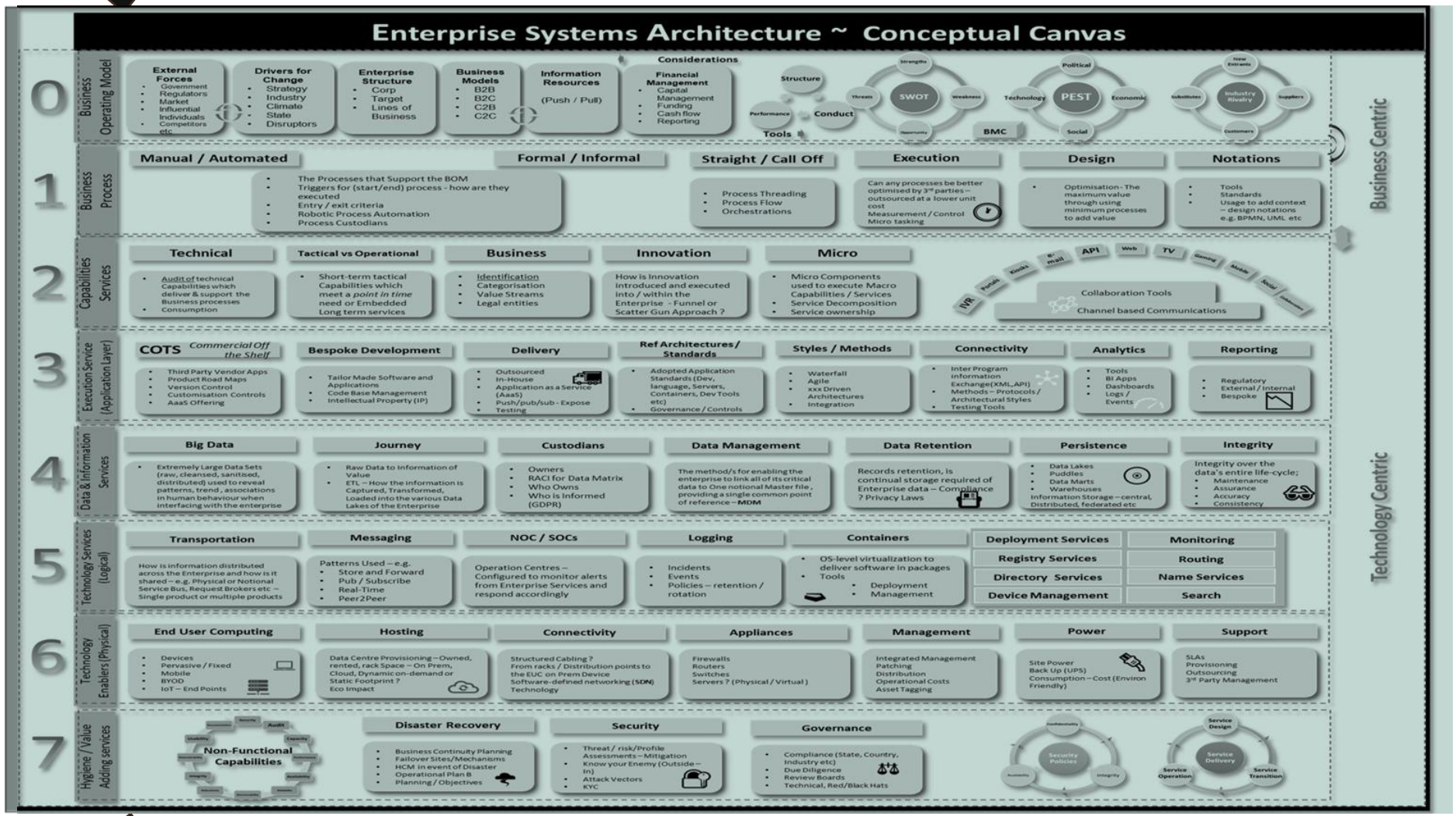
Banco Central do Brasil is responsible for supervising the compliance by all supervised entities with the provisions of **Law 9,613/1998**, which provides on prevention of money laundering and **terrorism funding** in the National Financial System (SFN).

Constantly Scan the Regulatory Authorities



Understanding your organisational the Business Operating Model

- Financial Regulatory Authority
- Anti-Money Laundering
- Bribery
- Consumer Protection
- AI
- Cloud Policies
- Data Privacy
- Fraud
- Company Registers
- Terrorism
- Freedom of Information
- Sanctions
- Misc.

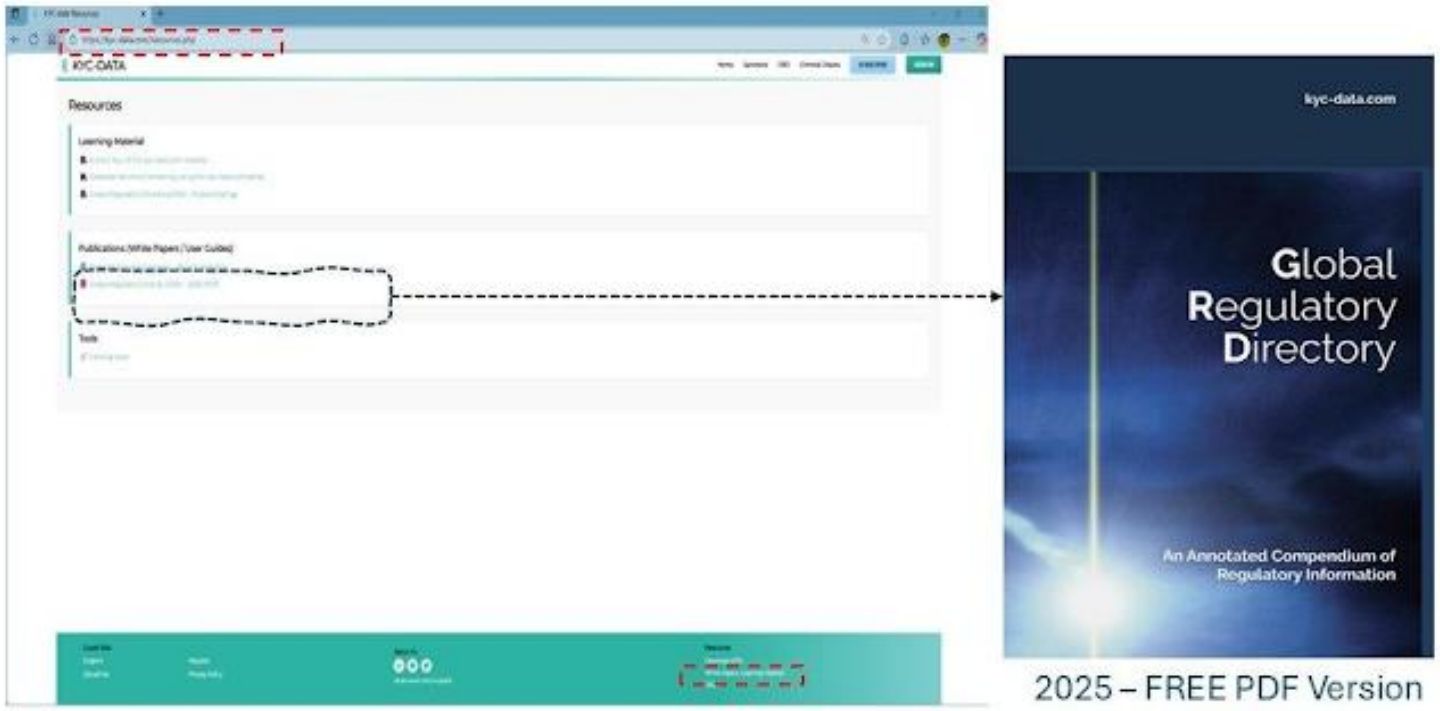


RESOURCE : FREE PDF Book !

The e-book version of the Global Regulatory Directory (GRD 2025) is no longer available for purchase as work continues on the 2026 version. However, the paperback is still available from Amazon

The good news is that the PDF version is now available FREE for download at the kyc-data.com portal where the Regulatory URLs are maintained.

Grab your FREE PDF COPY of the Global Regulatory Directory at https://kyc-data.com/docs/GRD_2025-PUBLIC-RELEASE.pdf - *no registration required*.



www.kyc-data.com Resources Page

Q&A

Thank You