



OPENING
DOORS TO
KNOWLEDGE
AND SKILLS

INTERNATIONAL COMPLIANCE FOUNDATION LEVEL



With the successive financial crises and adverse publicity, serious concerns have arisen forcing G24 governments and international organisations to “better” regulate / monitor the activities of banks and other financial institutions. In this context, the compliance function plays a key role in shaping the compliance culture of an institution.

A key role in shaping the compliance culture



This programme is constructed in 5 parts and is designed to provide participants with high level but practical insights into the genesis, evolution and key principles applicable to the compliance function.

It then looks at key regulatory topics to provide practical knowledge of regulations significantly impacting the operational activities of financial institutions.

**Highly
practionner
oriented teaching
methods**

Both the content of each parts and the teaching methods are highly practitioner oriented. Key regulations covering the financial firms are explained in a practical context during lectures delivered by accomplished compliance professionals.



Agenda

#1

COMPLIANCE, GENESIS & KEY PRINCIPLES

#2

COMPLIANCE FUNCTION FUNDAMENTALS

#3

FINANCIAL CRIME FRAMEWORK

#4

INVESTOR PROTECTION: MIFID OVERVIEW

#5

DATA PROTECTION



- COMPLIANCE, GENESIS & KEY PRINCIPLES
- COMPLIANCE FUNCTION FUNDAMENTALS
- FINANCIAL CRIME FRAMEWORK
- INVESTOR PROTECTION : MIFID OVERVIEW
- DATA PROTECTION

COMPLIANCE, GENESIS & KEY PRINCIPLES



COMPLIANCE, GENESIS & KEY PRINCIPLES

Agenda

1. Introduction – Why Compliance ?

- 1.1 Genesis and evolution
- 1.2 Compliance, ethics and governance

2. What is Compliance ?

- 2.1 Definition and objectives
- 2.2 Compliance risks
- 2.3 Compliance laws, rules and standards
- 2.4 Hierarchy of norms

3. International bodies promoting Compliance

- 3.1 Basel Committee on Banking Supervision
- 3.2 European Commission & European Supervisory Authorities (ESAs)
- 3.3 FATF / GAFI
- 3.4 Wolfsberg Group
- 3.5 Organisation for economic cooperation and development (OECD)



1. Introduction : Why Compliance ?





1.1 Genesis (1/2)

**An unstable
geopolitical
environment** in
a globalized
economy

- 1970 USA~ major business and government excesses generate legal, public and political reaction.
- SEC investigations discovered a number of US companies participated in overseas bribery.
- International sanctions, restrictions and embargoes are used politically in the foreign policies.
- Fight against money laundering and terrorist financing.
- Globalisation of economies in the context of fast exchange of information involved new risks: external fraud, cyber-fraud, financial crime, etc.





1.1 Genesis (2/2)

Development of
**Corporate
Social
Responsibility
and ethics**

- White collar crime shows strong growth (abuse of corporate assets, abuse of weaknesses, bankruptcy, fraud with the grants or the issue of CO2 quotas, market abuse, manipulation or interest rates, etc.)

**A highly
regulated
industry**

- Media pressure, NGOs, the consumers...
- A regulatory “tsunami” ... Development of “class actions” in Europe



How did the financial crises effect the regulatory environment, development, expansion and the growth of the risks of non-compliance and reputation?

1.2 Evolution

Banking and financial crises: loss of trust in financial institutions



Economic crises



Budgetary and Regulatory crises

Strengthening of international rules and increasing transparency and INTEGRITY of markets, protection of investors and consumers of financial instruments.

At the European level, the European Commission published and updated Directives/Regulations which find their source in the "consumer protection" package: MiFID2/MIFIR, PRIIPS, Directive Intermediation of Insurance "IMD2", Directive Transparency, MAD/MAR, EMIR, AIFMD, AML I,II,III, IV, V, VI Directives

Economic crises tend to encourage the development, expansion, and growth of the risk of fraud or the violation of the rules, white collar crime or "financial crime"...

The budgetary crises in occidental Countries encouraged governments to reinforce pressure and the development of tax matters regulations: US FATCA, CRS, BEPS... In this context, tax crime is a key subject of 4th AML Directive AML (primary offence of money laundering). 2019 Implementation of 5th AML Directive which tends to go farther than international AML/CFT standards (High risk countries list/ UBOs)



2. What is Compliance ?





2.1 Definition and Objectives



Compliance can be defined as the process by which a business ensures that it has fulfilled all of its regulatory and statutory obligations.

It refers to processes which make it possible to ensure respect for the norms applicable to the business by **all employees including executive management, Board of Directors** and also the values the ethical spirits inculcated by management of the institution.

The aim of the Compliance function is:

- to anticipate
 - to identify
 - to assess
- } the **compliance risks** of an institution
- and to **assist the executive management/employees** in limiting these risks,
 - by **monitoring** them on an **on-going basis** and without delay



2.2 Compliance risks

Basel Committee : compliance in banks, 2005:



“risk of legal or regulatory sanctions, material financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organisation standards, and codes of conduct applicable to its banking activities (together, “compliance laws, rules and standards”)”

- reputation risk
- legal risk
- risk of dispute
- risk of sanctions
- operational risk aspects

All the activities of the institution **and** on a cross-border basis



2.3 Compliance laws, rules and standards

- Laws & regulations
- Rules & standards
- Market conventions
- Codes issued by professional associations
- Internal codes of conduct
- Etc.



2.4 Importance of Ethics

Professionals must ensure their firm complies not only with the ***letter*** but also the ***spirit*** of the law and regulatory ***expectations***.

Compliance professionals must always perform their daily work by having in mind the importance of Ethics.





2.5 Principles

A financial institution's reputation relies on a strict observance of the rules (legal, professional, contractual,...) as well as on an honest, responsible and ethical attitude adopted by all its employees.

The Code of Ethics sets the principles and values which the institution considers to be fundamental in its relations with all its stakeholders :

- Employees, Clients, Market
- Suppliers, Shareholders
- Regulators, other third parties, etc.

It provides the reference framework within which all staff members are to perform their activities



Code of Conduct - Key expectations

- **Loyalty, Fairness and Integrity:** A firm shall act with loyalty, fairness and integrity in their relations with customers, other financial sector professionals, markets and society in general.
- **Competence, Care and Diligence:** A firm shall act with diligence and care in relation to the services provided by them. They must have the resources and procedures required to implement their activities effectively.
- **Respect for Privacy and Confidentiality:** A firm shall strictly respect the duty of confidentiality and discretion in regard both to customers and third parties.
- **Compliance with Laws and Regulations:** A firm shall faithfully and rigorously comply with the letter and the spirit of the norms and rules applicable in the performance of their duties.
- **Security and Reliability:** A firm shall ensure to protect the security of assets entrusted to them and on the reliability of the services provided by them.
- **Sound and Efficient Governance:** A firm shall implement proper governance in the conduct of its activities.



Anti Bribery & Corruption



Bribery The offering, promising, giving, accepting or soliciting of an advantage as an inducement for an action which is illegal, unethical or a breach of trust. Inducements can take the form of gifts, loans, fees, rewards or other advantages (taxes, services, donations, favours etc.).

Corruption Generally speaking as “the abuse of entrusted power for private gain”. Corruption can be classified as grand, petty and political, depending on the amounts of money lost and the sector where it occurs. Grand corruption consists of acts committed at a high level of government that distort policies or the central functioning of the state, enabling leaders to benefit at the expense of the public good. Petty corruption refers to everyday abuse of entrusted power by low- and mid-level public officials in their interactions with ordinary citizens, who often are trying to access basic goods or services in places like hospitals, schools, police departments and other agencies.



Particular attention to :

- Transactions with countries that rate high on the Corruption Perceptions Index ;
- Transactions with Political Exposed Persons ;
- Transactions involving government/public contracts ;
- NPOs (Non-Profit Organizations) and Charities. as per FATF Recommendation 8

Avoidance of Bribery & Corruption

- Policy and procedure for on-boarding of exposed clients or countries
- Conflicts of interest/gifts and business entertainment
- Monitoring of transactions (cf. sensitive employees/clients)



Whistleblowing



Whistleblowing is when an employee reports suspected wrongdoing at work ('disclosure in the public interest') outside the usual escalation route. An employee can report any act, process or behaviour that is not right, is illegal or if anyone at work is neglecting his duties, including (but not limited to):

How ?

- by encouraging staff to make disclosure of criminal or unethical conduct
- by ensuring that disclosure will be treated with discretion and utmost confidentiality
- by ensuring that disclosure can be submitted by staff on an anonymous basis
- by explicitly protecting the individual against dismissal or other adverse treatment when they make a disclosure in good faith

- a criminal offence ;
- the company not obeying the law ;
- covering up wrongdoing.

Whistleblowing Procedure

Ensures that all members of staff can *whistle-blow* (even anonymously), on (suspected) criminal or unethical conduct.



Professional Secrecy (1/2)



Confidential information is :

- All information related to the institution itself that has not been made public (including internal memos, policies, credit applications, employee and supplier data)
- All non-public information about existing and prospective clients
- Assumption that all information to be confidential unless it has clearly been made public
- The more staff have knowledge of the confidential information, the more risk there is that confidentiality will be breached. Therefore, always remember: “Need to know” principle!



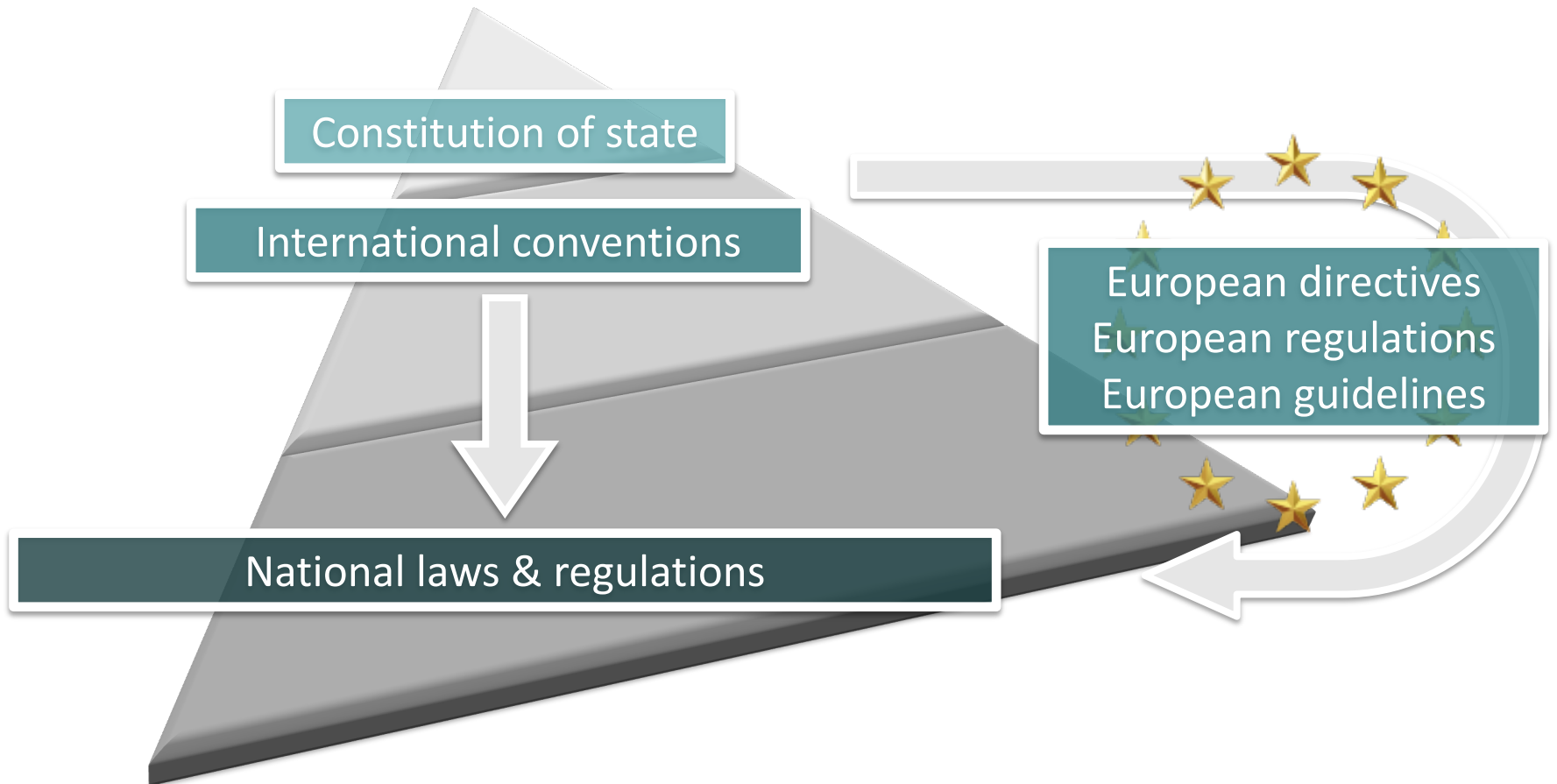
Professional Secrecy (2/2)

General obligations for confidentiality :

- Professional secrecy (should not be confused with the banking secrecy) has not disappeared but **exceptions under strict rules possible** (regulators, request for specific information between tax authorities based on bilateral agreements,...).
- **Continuity of the secrecy obligation** after leaving the institution.
- Continuity of the secrecy obligation towards clients that have closed the account or business relationship.



Hierarchy of Norms





3. International Bodies Promoting Compliance





3. International Bodies Promoting Compliance

STRONG AND DEEP INFLUENCE ON
ALL COMPLIANCE REGULATIONS

3.1 Basel Committee on Banking Supervision

www.BCBS.org/bcbs

3.2 European Commission and European Supervisory Authorities

<https://ec.europa.eu> www.eba.europa.eu
<https://eiopa.europa.eu> www.esma.europa.eu

3.3 FATF / GAFI

www.fatf-gafi.org

3.3

3.4 Wolfsberg Group

www.wolfsberg-principles.com

3.4

3.5 Egmont Group <https://egmontgroup.org>

3.5

The Organisation for Economic Co-operation and Development (OECD)

www.oecd.org



3.1 Basel Committee on Banking Supervision (1/5)

What ?

- Founded in 1974 by the G-10 central bank governors.
- Now the Basel Committee on Banking Supervision (BCBS) has the mission of fostering discussion and facilitating collaboration among central banks.
- Its mandate is to strengthen regulation, supervision and best practices of banks worldwide with the purpose of promoting financial stability.
- Its 45 members comprise central banks and bank supervisors from 28 jurisdictions (2019).



3.1 Basel Committee on Banking Supervision (2/5)

Activities

- Exchanging information of developments in banking sector and financial markets, to help identify current or emerging risks;
- Sharing supervisory approaches and techniques to promote common understanding and improve cross-boarder cooperation;
- Establishing and promoting global standards, guidelines and sound practices;
- Filling regulatory and supervisory gaps that pose risks to financial stability;
- Monitoring the implementation of BCBS standards in member countries, thus contributing to a “level playing field”;
- Consulting with central banks and bank supervisory authorities which are not members of BCBS, promoting implementation of standards, guidelines, sound practices;
- Coordinating and cooperating with other financial sector standard setters and international bodies.



3.1 Basel Committee on Banking Supervision (3/5)

How ?

- **Through groups**, working groups, virtual networks and task forces
- **Policy dissemination**: policy decisions by the Basel Committee are published in the form of:
 - **Standards** : The BCBS expects full implementation of its standards by BCBS members and their internationally active banks. However, BCBS standards constitute minimum requirements and BCBS members may decide to go beyond them.
 - **Guidelines** : Generally supplement BCBS standards by providing additional guidance for the purpose of their implementation.
 - **Sound practices** : Describe actual observed practices, with the goal of promoting common understanding and improving supervisory or banking practices.



3.1 Basel Committee on Banking Supervision (4/5)

Main principles for Compliance function (1/2)

- Banking Supervisors must be convinced that effective Compliance policies and procedures are followed and that management take appropriate corrective action when compliance failures are identified.
- Compliance should be part of the culture of the organisation; it is not just the responsibility of the compliance staff.
- A bank should organise its compliance function and set priorities for the management of its compliance risks in a way that is consistent with its own risk management strategy and structures.
- Regardless of how the compliance function is organised within a bank, it should be independent and sufficiently resourced, its responsibilities should be clearly specified, and its activities should be subject to periodic and independent review by the Internal Audit function.

NB : BCBS recognizes the application of the proportionality principle depending on the size, nature, complexity and risks of each bank.



3.1 Basel Committee on Banking Supervision (5/5)

Main principles for Compliance function (2/2)



The Board of Directors is responsible for overseeing the management of the firm's compliance risks. The Board should **approve the compliance policy**, including a formal document establishing a permanent and effective compliance function. At least once a year, the Board should **assess** the extent to which the firm is effectively managing its compliance risks.



Senior Management is responsible for:

- the effective management of the bank's compliance risk,
- establishing and communicating the compliance policy;
- ensuring that it is adhered to; and
- reporting to the Board of Directors on the effective management of the compliance risk.



In case of **cross-border groups** : The compliance function and its responsibilities should be consistent with local legal and regulatory requirements



Role of **supervisors**



3.2 European Commission & European Supervisory Authorities (ESAs) (1/9)

Roles and Responsibilities

The European Commission

- **Legislation initiative** : Proposal to the Council and to the European parliament of any legislative proposals : regulations or directives
- **Legal instruments** : implementing & delegated acts
- **Enforcement** : Once legislation is passed by the Council and Parliament, it is the Commission's responsibility to ensure it is implemented (sanctions)
- Power to make **recommendations** or deliver **reports** and **opinions**

The Commission is collectively accountable to the European Parliament



3.2 European Commission & ESAs (2/9)

European System of Financial Supervision (ESFS)

Established in consequence of the reform to the structure of supervision of the financial sector in the EU. Before and during the **financial crisis in 2007 and 2008**, the European Parliament had called for more integrated European supervision in order to ensure a true level playing field for all actors at the level of the EU and to reflect the increasing integration of financial markets in the Union.

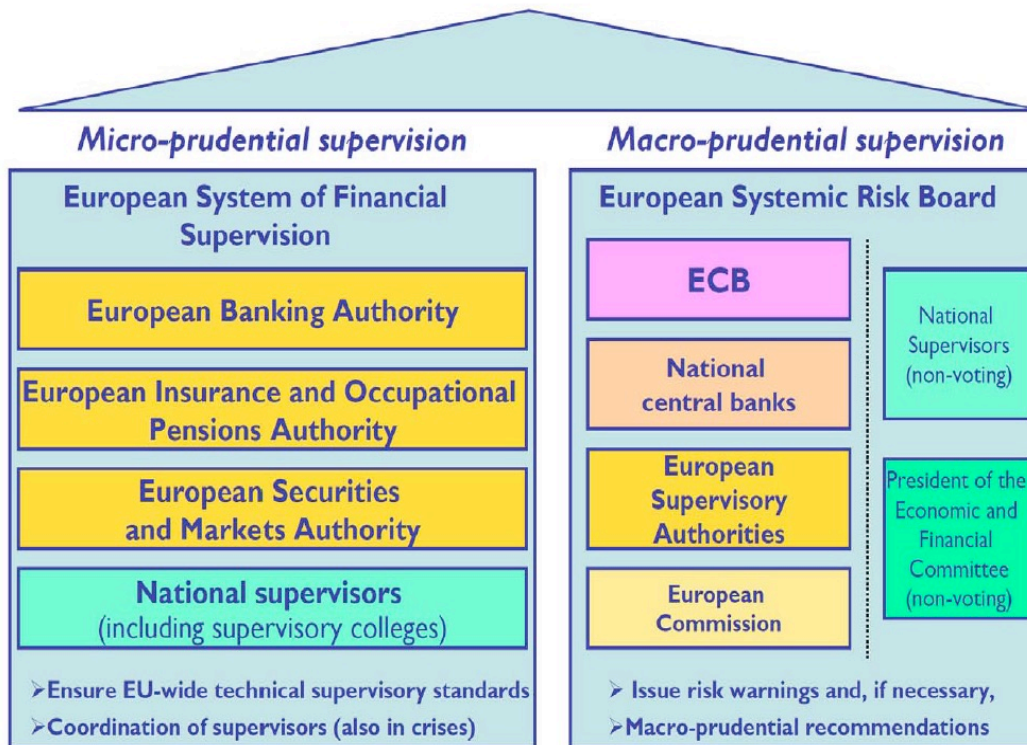
As of 1st January 2011,

The ESAs are :

- **European Banking Authority (EBA)**
- **European Insurance and Occupational Pensions Authority (EIOPA)**
- **European Securities and Markets Authorities (ESMA)**
- **Joint Committee of the ESAs**
- **European Systemic Risk Board (ESRB)**



New supervisory framework in the EU



Source: Papademos (2010)



3.2 European Commission & European Supervisory Authorities (ESAs) (4/9)

ESA tasks

- harmonising financial supervision in the EU by developing a single rulebook and set of prudential standards;
- helping to ensure the consistent application of the rulebook to create a level playing field;
- mandated to assess risks and vulnerabilities in the financial sector.

ESAs are accountable to the EU Parliament, Council and Commission.



3.2 European Commission & ESAs (5/9)

3.2.1 EBA (European Banking Authority)

Roles and Responsibilities

- ensure effective and consistent level prudential regulation as well as supervision across European banking sector;
- maintain EU financial stability;
- safeguard the integrity, efficiency and orderly functioning of the banking sector;
- improve the functioning of the internal market by ensuring appropriate, efficient and harmonised European supervision and regulation;
- contribute, through the adoption of Binding Technical Standards and Guidelines, during the creation of the European Single Rulebook in banking. The Single Rulebook aims at providing a single set of harmonised prudential rules for financial institutions throughout the EU, helping create a level playing field and providing high protection to depositors, investors and consumers.



3.2 European Commission & ESAs (6/9)

3.2.2 EIOPA (European Insurance and Occupational Pensions Authority)

Roles and Responsibilities

- Better protecting consumers and rebuilding trust in the financial system.
- Ensuring high, effective and consistent levels of regulation and supervision taking into account the varying interests of all Member States and the different nature of financial institutions.
- Greater harmonisation and coherent application of rules for financial institutions & markets across the European Union.
- Strengthening oversight of cross-border groups.
- Promoting coordinated EU supervisory responses.



3.2 European Commission & ESAs (7/9)

3.2.3 ESMA (European Securities and Markets Authority)

Roles and Responsibilities

- enhancing investor protection and promote stable and orderly financial markets
- assessing risks with regard to investors, markets and financial stability
- completing a single rulebook for EU financial markets
- promoting supervisory convergence: issuing guidelines, opinions, technical standards
- directly supervising specific financial entities: credit rating agencies, trade repositories



3.2 European Commission & ESAs (8/9)

3.2.4 ESAs Joint Committee

Roles and Responsibilities

- **Strengthen cooperation** between ESAs and develops consistency in practices
- **Micro-prudential analyses:** cross sector developments, risks and vulnerabilities for financial stability, retail investment products, supervision of financial conglomerates, accounting and auditing, and measures combating money laundering & terrorist financing
- The ESAs, within the Joint Committee, jointly **explore and monitor potential emerging risks** facing market participants and the financial system as a whole.
- The Joint Committee plays an **important role in the exchange of information** with the European Systemic Risk Board (ESRB) and in developing the relationship between the ESRB and the ESAs.



3.2 European Commission & ESAs (9/9)

3.2.5 ESRB (European Systemic Risk Board)

Roles and Responsibilities

- Macro-prudential oversight of the financial system within the Union in order to contribute to the prevention/mitigation of systemic risk to financial stability in the Union
- Determining, collecting and analysing all the relevant and necessary information;
- Identifying and prioritising systemic risks;
- Issuing warnings where such systemic risks are deemed to be significant and, where appropriate, making public warnings;
- Issuing recommendations for remedial action in response to the risks identified and, where appropriate, making those recommendations public;
- Monitoring follow-up to warnings and recommendations;
- Cooperating closely with all the other parties to the ESFS;
- Coordinating its actions with those of international financial organisations, as well as the relevant bodies in third countries on matters related to macro-prudential oversight



3.3 FATF (Financial Action Task Force)

- An inter-governmental body established in 1989 located in Paris
- **Objectives** : to set standards, to promote effective implementation of legal, regulatory and operational measures for AML/CTF/ PF
- Is a “**policy-making body**” which works to generate the necessary political will to bring about national legislative and regulatory reforms.
- **FATF recommendations**: First issued in 1990, they were last revised in 2012 : 40 recommendations on AML/CTF/ PF
- **Monitoring of peer reviews**: 4th round of mutual evaluations had begun in 2014
- **Publishing of typologies** of ML/TF techniques & trends, risk based approach guidance

Members (38 in 2019) & associate members through FSRBs : FATF style-regional bodies & Observers e.g. Basle Committee, United Nations, IOSCO, etc.



3.4 Wolfsberg Group (Think Tank)

- Starting in 2000, the Wolfsberg Group is an association of 13 global banks which aim to develop frameworks and guidance for the management of financial crime risks, particularly with respect to Know Your Customer, AML/CTF policies.
- It has since developed a large range of standards, also focused on other financial crime risks, such as corruption, terrorist financing and sanctions.
- The Wolfsberg Group has neither a written constitution nor any formalized set of rules or statutes. It has developed its practices and procedures over time.
- Wolfberg Standards (PEPs, Private Banking, Payment transparency, anti bribery and corruption, trade finance ...)
- Wolfsberg Correspondent Banking Due Diligence Questionnaire (updated 2018)

Members : Banco Santander, Bank of America, MUFG Bank, Barclays, Citigroup, Crédit Suisse, Deutsche Bank, Goldman Sachs, HSBC, J.P. Morgan Chase, Société Générale, Standard Chartered Bank, UBS.



3.5 Egmont Group

- The Egmont Group is a united body of **164 Financial Intelligence Units (FIUs)**.
- It provides a platform for the secure exchange of expertise and financial intelligence to combat money laundering and terrorist financing (ML/TF)
- This is especially relevant as FIUs are uniquely positioned to cooperate and support national and international efforts to counter terrorist financing and are the trusted gateway for sharing financial information domestically and internationally in accordance with global Anti Money Laundering and Counter Financing of Terrorism (AML/CFT) standards.
- It has since developed a large range of standards, also focused on other financial crime risks, such as corruption, terrorist financing and sanctions.
- The Group meets regularly at the Egmont Arenberg Palace in Brussels, Belgium.



3.6 OECD : Organisation for Economic Cooperation and Development (1/2)

- Established in 1961, headquartered in Paris, 36 member countries
- Forum for governments to share experiences and seek solutions to common problems.
- International standards on a wide range of things, from agriculture and tax to the safety of chemicals
- Compliance topics : **TAXATION**
- OECD helps countries so that their own tax systems work for them.
- SCOPE : international and domestic issues, across direct and indirect tax matters, tax transparency – ensuring that bank secrecy and other forms of financial opacity do not prevent tax administrations from being able to apply their tax laws no matter where their taxpayers choose to place
- Global Forum on Transparency and Exchange of Information for Tax Purposes (Global Forum)



3.5 OECD : Organisation for Economic Cooperation and Development (2/2)

- 150 members of the Global Forum on Transparency and Exchange of Information for Tax Purposes
- 115 countries and jurisdictions in the Inclusive Framework on BEPS (Base Erosion and Profit Shifting)
- 120 countries and jurisdictions participating in the multilateral Convention on Mutual Administrative Assistance in Tax Matters
- 80 countries and jurisdictions, accounting for more than 1 360 bilateral tax treaties, have signed the Multilateral Convention to Implement Tax-Treaty Related Measures to Prevent BEPS
- 100 countries and jurisdictions committed to automatically exchanging financial account information by September 2018
- Compliance related topics : FATCA, CRS : Common Reporting standards; Transfer pricing, anti-tax avoidance directive (ATAD), etc.



DO
GO
THING
GOOD
GOOD
GOOD

- COMPLIANCE, GENESIS & KEY PRINCIPLES
- COMPLIANCE FUNCTION FUNDAMENTALS
- FINANCIAL CRIME FRAMEWORK
- INVESTOR PROTECTION : MIFID OVERVIEW
- DATA PROTECTION

COMPLIANCE, FUNCTION FUNDAMENTALS



COMPLIANCE, FUNCTION FUNDAMENTALS

Agenda

1. Establishing a Compliance function

- 1.1 Compliance part of the Internal Control Framework
- 1.2 Compliance requirements

2. Key compliance responsibilities

- 2.1 Compliance responsibilities
- 2.2 Compliance topics
- 2.3 Risk based approach ('RBA') concept

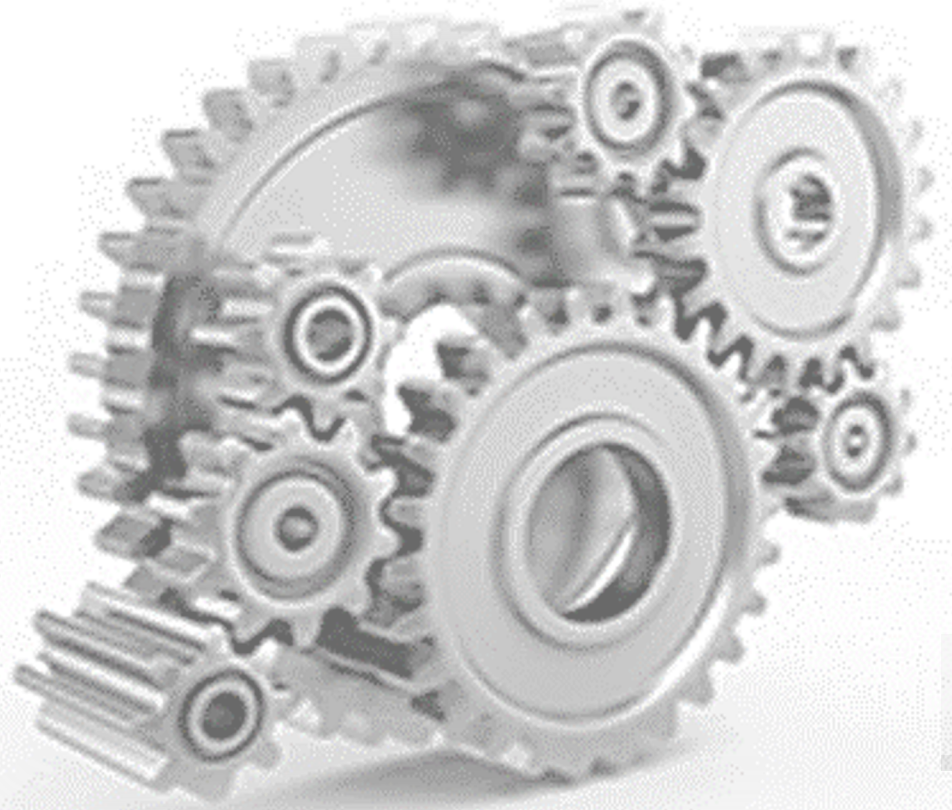
3. Actors: roles and responsibilities

- 3.1 Board of Directors
- 3.2 Executive Management
- 3.3 Employees
- 3.4 Compliance Function
- 3.5 Relationships with other key functions/stakeholders

4. Compliance founding documents



1. Establishing a Compliance function





1.1 Compliance, part of Internal Control Functions

- Internal control function
- The three-lines-of-defence model

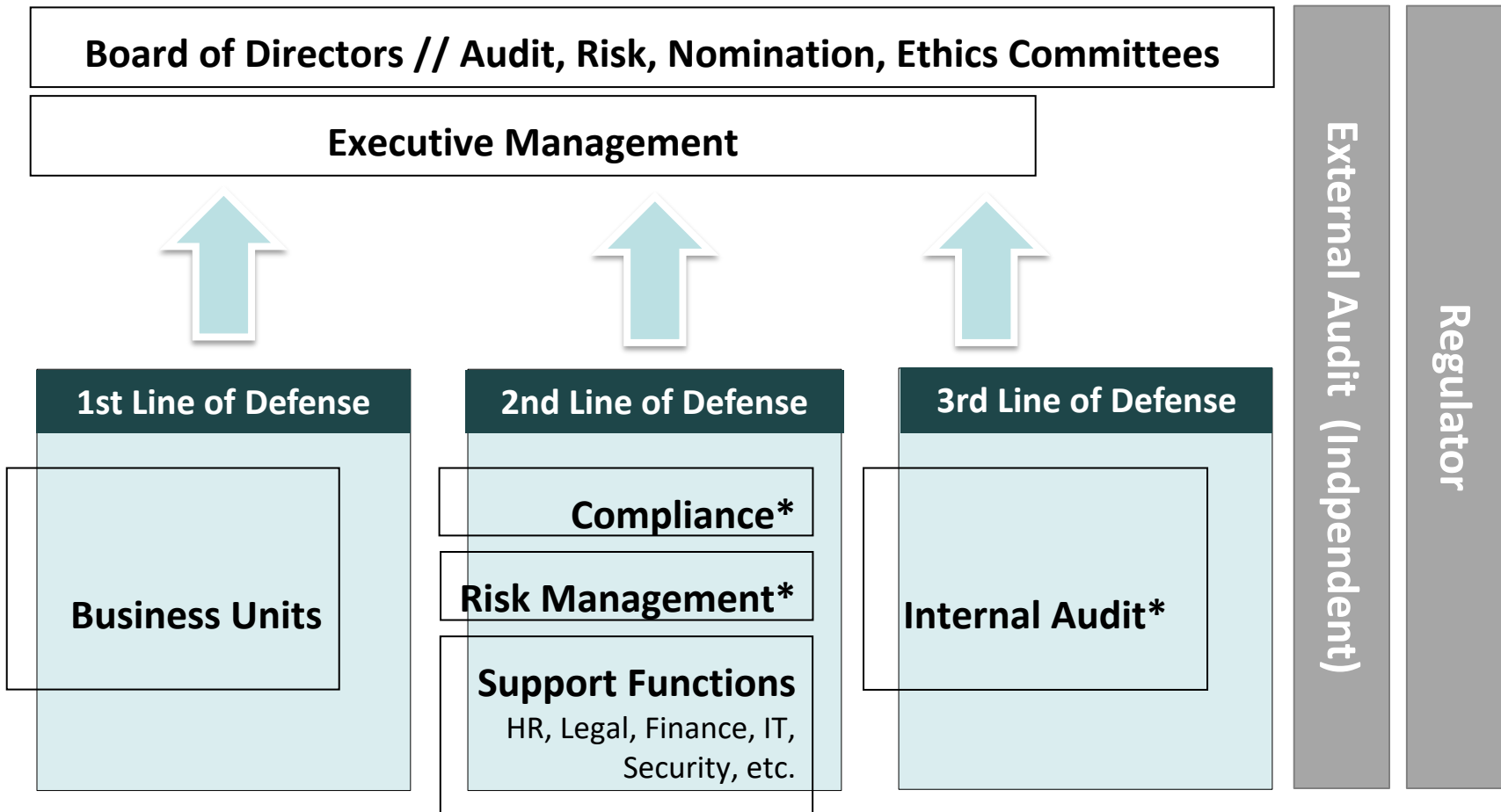


- Each shall be under the responsibility of a separate head of function, even though some exceptions might be authorised following the principle of proportionality.
- Internal audit and compliance can never be assigned to the same person.





1.2 The Internal Control framework



* Report also to the Board of Directors



1.3 Compliance requirements (1/2)

1.3.1. Stature of the function

- Appropriate standing, authority and independence
- Access to information, personnel
- Resources : sufficiency, adequacy, competence
- Chief Compliance Officer for Banks (CCO) subject to regulators' approval in the EU: high degree of professional qualification and good knowledge of laws, rules and standards -
- Proportionality principle : a full time position of CCO is not mandatory, but another decision is subject to regulator approval in the EU





1.3 Compliance requirements (2/2)

1.3.2. Independence of the function

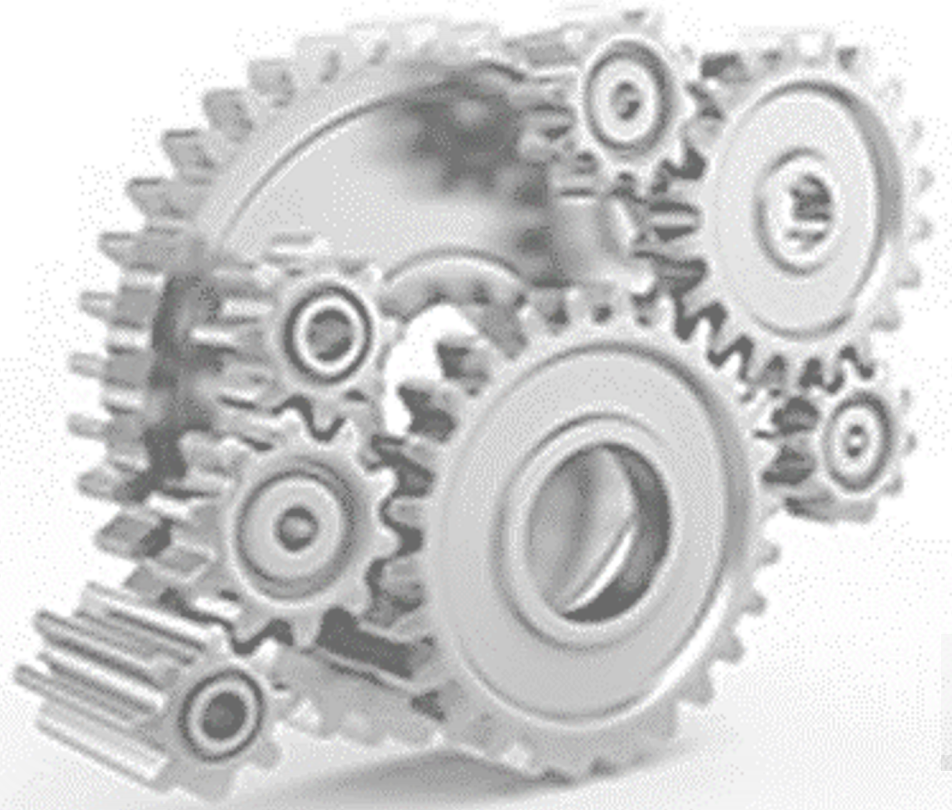
- Function is independent from management to avoid undue influence or obstacles as that function performs its duties. (Basle committee, 2015)
- The compliance function should directly report to the board. (Basle committee, 2015)
- Conflicts of interest management

1.3.3. Permanence of the function

- No external outsourcing is allowed for banks
- But possible recourse to external experts
- Specific tasks of the compliance function may be outsourced in the institution, but they must remain subject to appropriate oversight by the head of compliance (principle 10 of 2005 Basel committee guidelines)



2. Key Compliance Responsibilities





2.1 Compliance responsibilities (1/3)

2.1.1. Effective management of Compliance Risks

- Identify, measure, mitigate, monitor
- Before new activities, products or business relationships, transactions and network of the group at international level
- Cooperation with risk management

2.1.2. Advise the board and executive management

- Compliance with applicable laws, rules and standards
- Keep them informed of developments in the area

2.1.3. Guidance and Education

- Educate staff on compliance issues
- Handle compliance queries from staff members
- Provide guidance to staff on the appropriate implementation of applicable laws, rules and standards in the form of policies and procedures and other documents such as compliance manuals, internal codes of conduct and practice guidelines.



2.1 Compliance Responsibilities (2/3)

2.1.4. Monitoring & Testing

- Permanent and recurring obligations for financial institutions: Client on-boarding, targeted financial sanctions checks, private list checks , transaction monitoring, regulatory updates, risks assessment/mapping, training and reporting;
- To develop a compliance monitoring plan according to risk, resources (budget) and timeframe;
- The Compliance Monitoring Plan ('CMP') should take into consideration the organization of the actions and tasks, and distributing them between teams following an agenda including all necessary priorities and potential unforeseen events. It is then necessary to assess the budget and resources that are necessary to its realization. This also includes staff costs, specific software, operational costs, outsourced activities...

2.1.5. Statutory Role & Liaison with Authorities

- Responsible for AML/CTF matters
- Liaison with relevant regulators, standard settlers and external experts



2.1 Compliance Responsibilities (3/3)

MORE BROADLY:

**Support corporate values, policies and processes
to help ensure that the firm acts responsibly
and fulfils all applicable obligations**

**Ensure that the firm operates with integrity
and in compliance with applicable laws
rules and standards**



2.2 Compliance Topics (non-exhaustive list)

1. Fight against money laundering and terrorist financing: AML/CTF
2. Prevention in regard to market abuse and personal transactions
3. Integrity of financial markets
4. Protection of customer and investor interests
5. Personal data protection and observance of professional secrecy
6. Avoidance and management pertaining to conflicts of interest
7. Prevention of using the financial sector by third parties to circumvent their regulatory obligations
8. Management of compliance risks related to cross border activities
9. New products and new procedures compliance
10. Ethics, codes of conduct, professional misconduct
11. Internal or external fraudulent behaviour and breaches of discipline

... and more ...



2.3 Risk Based Approach

GOALS

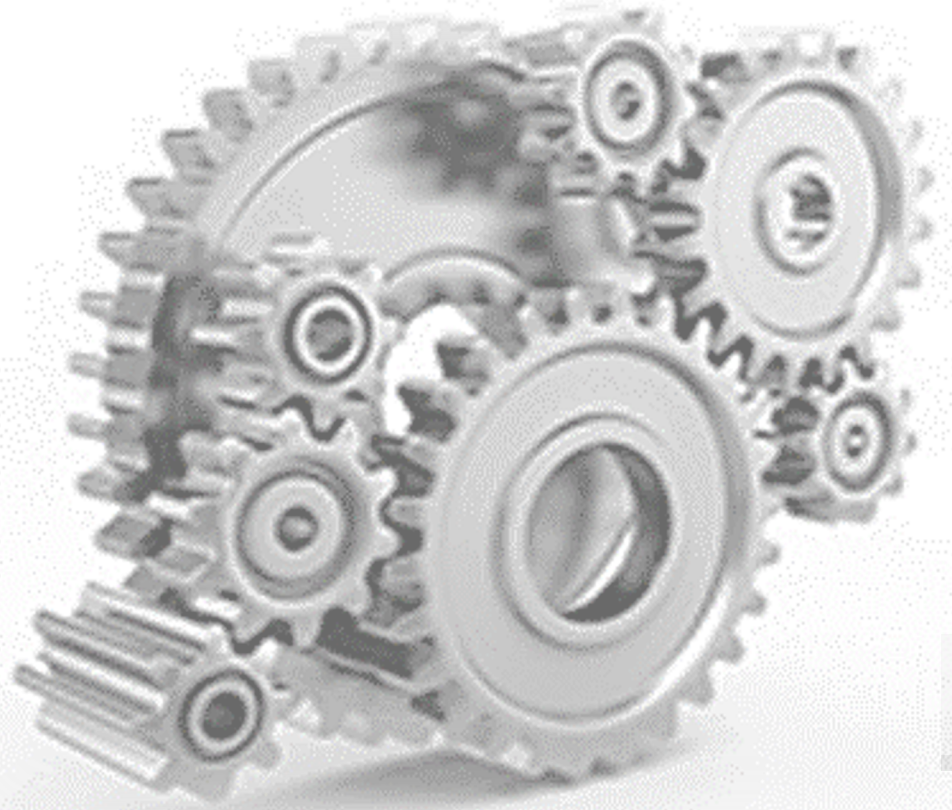
1. Highlighting the strengths and weaknesses of the financial institution facing its legal and regulatory obligations on an on going basis and without delay
2. Preventing immediate and long term impacts:
 - Potential sanctions, withdrawal of authorisation to carry on activities
 - Reputation (risk of image)
 - Litigation/dispute
 - Risk of financial loss (institution direct exposure or customers indemnification due to non respect of legal and regulatory requirements)
3. The corrective measures which should be documented in the Compliance Monitoring Plan
4. Efficiently allocate the compliance function's resources

**STRONG NECESSITY OF THOROUGH
RISK ASSESSMENT /MAPPING**

A large, hollow, downward-pointing arrow is positioned below the text box, indicating a flow or consequence from the text above.



3. Actors: Roles and Responsibilities





Roles and responsibilities at a glance





3.1 Board of Directors ('BoD')

The BoD shall have overall responsibility for the firm and shall ensure proper oversight of the compliance function. It shall:

- Receive regular reports on compliance matters and approve key documents such as:
 - Compliance Monitoring programme
 - AML/CFT policies/procedures
 - Compliance Charter
 - Annual control functions reports

- Appointment and dismissal of Chief Compliance Officer



3.2 Executive Management

- The Executive management is in charge of:
 - effective, sound and prudent day-to-day business
 - implementing internal written policies, procedures, strategies and guiding principles in relation to central administration and internal governance;
 - promotion of ethics and a sound compliance culture within the institution;
 - establishing the compliance function and proposing a Chief Compliance Officer;
 - drawing up and implementing the Compliance Charter;

- A senior manager should be responsible for control in respect to AML/CTF obligations (FATF recommendation 18)



3.3 Compliance Function

3.3.1 Role

- Implement compliance policy
- Identify and assess compliance risks, centralize and follow up compliance issues
- Identify applicable laws, rules and standards. Make an inventory available to staff. Ensure updates of the regulatory watch
- Implement a training and awareness program for staff and the Board regarding compliance topics
- Make periodic verifications that the rules in force are applied and make recommendations for remedial actions
- Document the work performed on compliance and report to the Board of Directors (Basle Committee 2015)



3.3.2 Example of work



1. Detect possible gaps in internal processes and policies with regard to new predicate offences of Money Laundering
2. Advise senior management and BoD of the possible gaps and recommend appropriate measures to become fully compliant with the new regulation
3. Update AML/CTF procedures including the new offences
4. Organise training sessions (e.g. update e-learning tools)
5. Integrate new controls in the CMP (new parameters in the AML tool or substantive tests)
6. Report to the Board on: control results, trend, specific risks identified and corrective actions when required



3.3.3 Relationships with Key Functions/Stakeholders

Within the institution

- Internal control functions
 - Internal Audit
 - Risk Management
- Business lines
- Key support functions
 - Tax
 - Legal
 - Human Resources
 - Accounting/Finance

Outside the institution

- External auditors
- Local or international regulators, and other authorities



Common objectives of control functions:

- strengthen the Internal Control framework,
 - identify and assess risks, review/challenge mitigating measures established by the firm
-
- Exchange reports on risks identified and incidents (audit reports, operational risks report, compliance reports...)
 - Share specific tools and methodologies (e.g. follow-up of action plans on audit issues), risk matrix, incidents inventory, etc.
 - Share and coordinate regulatory inventory
 - Operate through formal and informal meetings

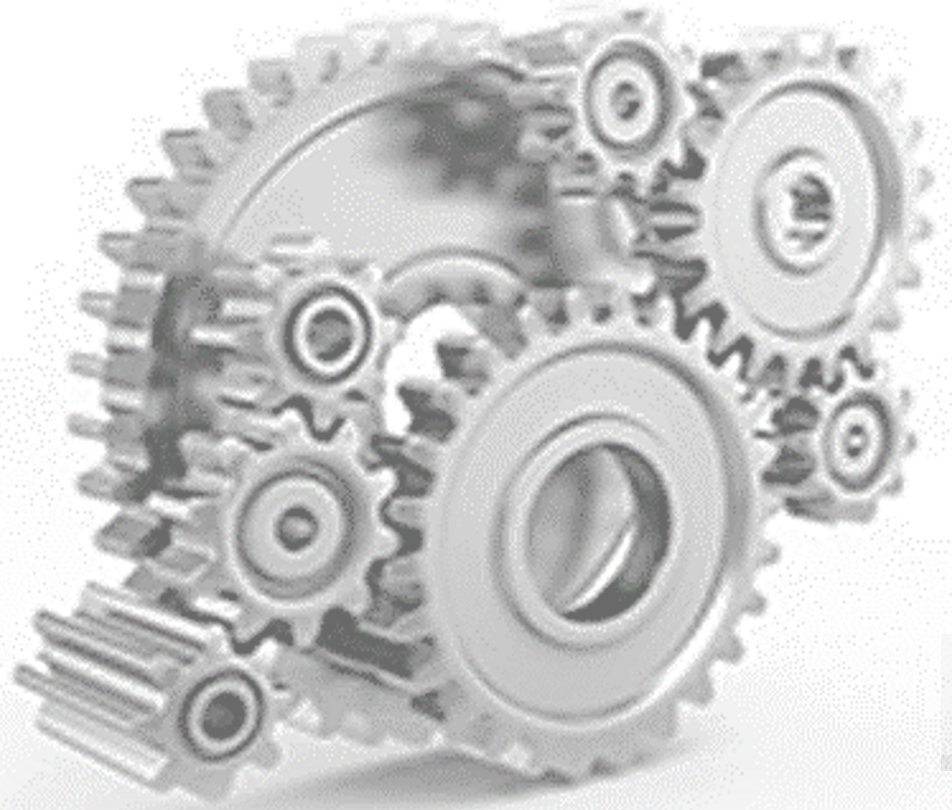


3.4 Employees

- All employees are individually responsible for complying with the compliance principles set out in the Compliance Charter, internal code of conduct, and complementary policies and procedures.



4. Compliance Founding Documents





4.1 Compliance Policy Key Components



Each financial institution has to put in place a Compliance Policy to be updated on a regular basis and to be approved by the Board of Directors

The Policy must :

- be in writing
- describe the relevant aspects of the compliance risk
- explain the principles, corporate values established by the BoD
- Implement the compliance function
- define its objectives and independency
- stipulate the creation of a Compliance Charter
- set up a continuous training program



4.3. Addendum : Further Reading : International

- ESMA Guidelines 2012/388 on certain aspects of MIFID compliance function requirements
- EBA internal governance EBA/GL/2017/11 dated 26/9/2017
- FATF recommendations, and relevant FATF publications : e.g : criminalising terrorist financing; counter proliferation financing, Risk Based Approach Guidance relating to banking sector, securities sector, etc.
- Basel committee :
 - April 2005: Guidelines : Compliance and the Compliance function in banks
 - August 2008: Survey on the implementation of the Compliance principles
 - January 2014: Sound management of risks related to ML/TF , revised in 2016 & 2017 - including exhibits on account opening and on correspondent banking
 - July 2015 : Corporate Governance principles for banks





- COMPLIANCE, GENESIS & KEY PRINCIPLES
- COMPLIANCE FUNCTION FUNDAMENTALS
- FINANCIAL CRIME FRAMEWORK**
- INVESTOR PROTECTION : MIFID OVERVIEW
- DATA PROTECTION

Financial Crime Framework



Agenda

1. Anti-Money Laundering (AML)
Counter Terrorism Financing (CFT) overview
2. Tax reporting overview – FATCA/ CRS
3. Predicate offence : Market abuse
4. International sanctions

FINANCIAL CRIME FRAMEWORK



1. **Anti-Money Laundering (AML) / Counter Terrorism Financing (CTF) overview**



1. INTRODUCTION





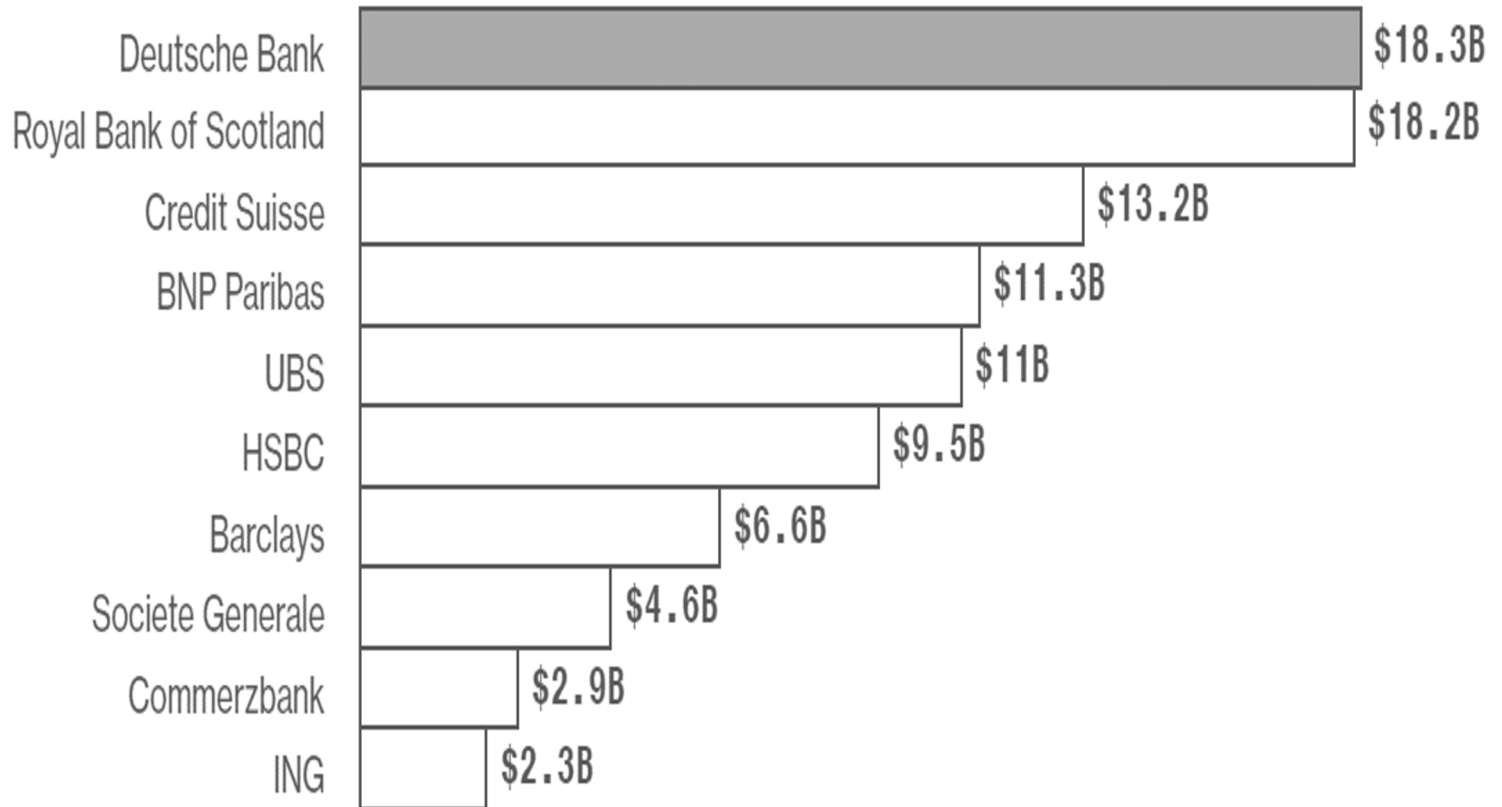
Combating financial crime

With the successive financial crises and adverse publicity, serious concerns have arisen forcing G24 governments and international organisations to “better” monitor/regulate the activities of banks and other financial institutions. In this context, combating financial crime is at the heart of regulatory and supervisory activities.

‘*Zero tolerance*’ against professionals not meeting best practice expectations appears to be the current trend for most regulators...

The cost of bad behavior

European banks with more than \$2 billion in fines and legal settlements paid, 2008-2018





The Zero Tolerance Approach



In recent years the CSSF has also applied a 'zero tolerance' approach towards financial crime and imposes fines on many local banks

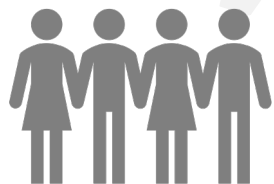
- Rothschild bank → €9 million
- Havilland → €4 million
- BIL → €4.6 million
- Etc...

At the European level, several actions have been taken to strengthen the European AML framework

The Danske Bank scandal is one of the largest money laundering scandals in European history



Dankse bank: What went wrong ?



> \$200 bn
> 12 years

Russia
Latvia
Cyprus
>150 countries

Estonia

Denmark



- Correspondent banks ?
- National Regulatory actions ?
- Action/Decision of EBA ?
- US action ?
- New EU AML framework → ECB role

- Weak AML controls
- \$29bn GDP/Estonia
- \$327bn GDP/DN
- Failure in KYC Non-resident portfolio
- Several high risk clients
- UBOs/SoWs not properly identified

The Outlook for Dankse Bank

- Potential penalties from both European and United States authorities
- \$2.7 billion created as a capital buffer to absorb potential fines
- There is great uncertainty over potential fines: Goldman Sachs estimated \$6 billion before core capital against the pillar 1 requirement is threatened. Jyske Bank analysts/ \$6.2bn-\$7.8bn in fines globally.
- However, fines may be the least concern in this worst scenario. The US Treasury could order banks that clear dollars on behalf of Danske to stop. That is what it did in February 2019 in the case of ABLV.
- Takeover risks...

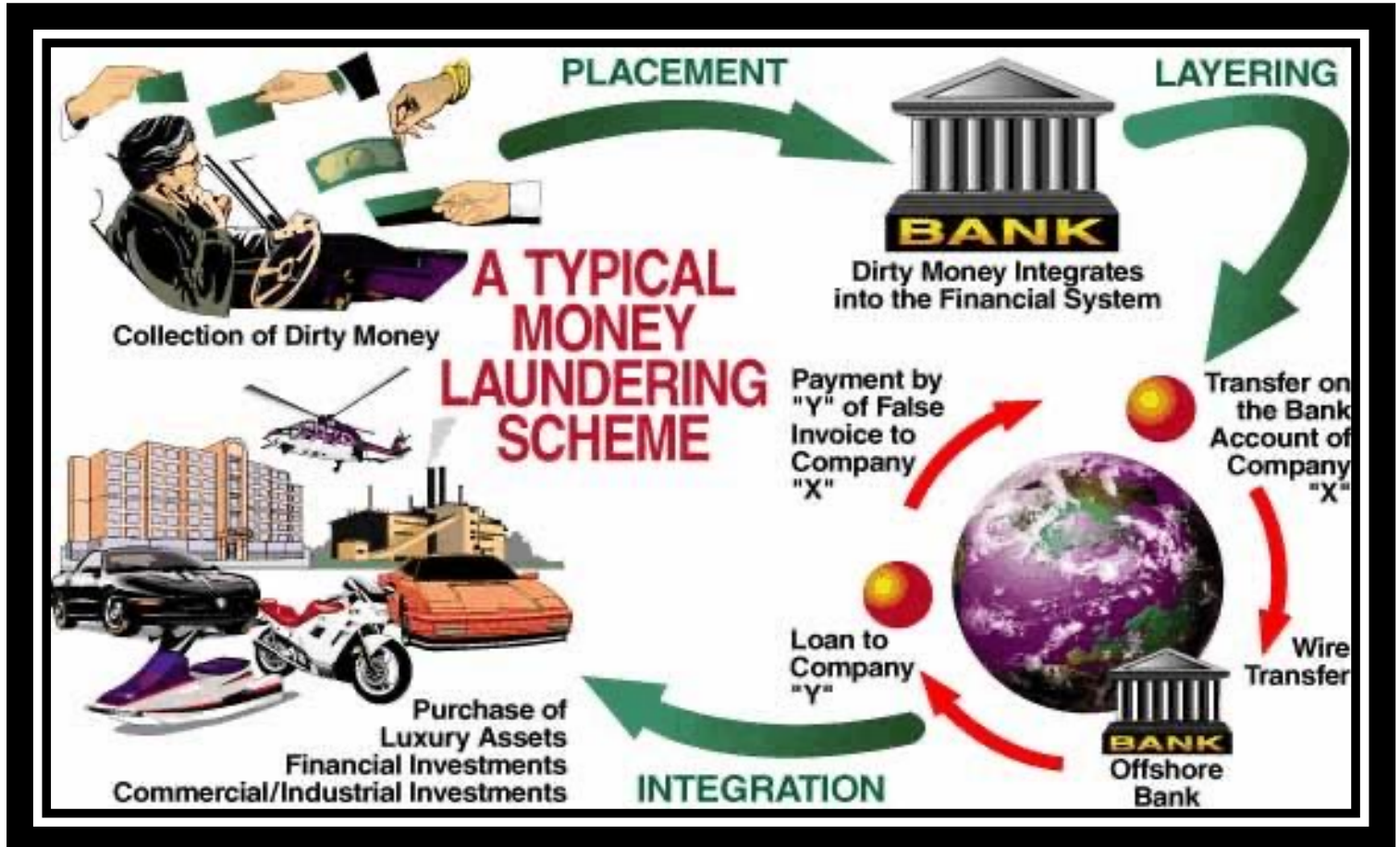


EU Finance Ministers Statement 4 November 2020

- Setup an EU agency that would fight money laundering across the EU
- Direct supervisory powers over a selected number of high-risk obliged entities
- Harmonise EU AML/CFT rules → Regulation versus Directive approach?
- Coordination and support for national Financial Intelligence Units
- Authority to take over supervision from a national supervisor in clearly defined and exceptional situations
- Expected Timeline: Q2-2021



1.1 What is Money Laundering ('ML')?





Definition of Money Laundering



Under Luxembourg Law, Money Laundering is defined in Art. 506.1 of the Penal Code:

‘..persons who have knowingly facilitated, by any means, the false justification of the nature, origin, location, disposition, movement or ownership of assets stemming from a range of “predicate offences”..’



Practical definition:

Money laundering can be defined as the processing of criminal proceeds to disguise the true origin and ownership. Money Laundering is the process by which illegally obtained funds (**‘dirty money’**) is given the appearance of having legitimately been obtained (**‘clean money’**)

Concept origin : Chicago Laundrettes/ “Prohibition”- 1930



Practical implications of Money Laundering



- **Knowingly facilitating**, by any means, the misleading justification of the nature, origin, location, mobility or ownership of goods, constituting the direct or indirect object or product of a primary offence (i.e. including any offence sanctioned by imprisonment of at least six months)
- **Knowingly helping** by the investment, the dissimulation, the disguise, the transfer or the conversion of goods originated from a primary offence
- **Acquiring**, detaining or using goods while knowing that these goods come from a primary offence
- **Attempting** to commit one of the above offences



The Three Stages of Money Laundering



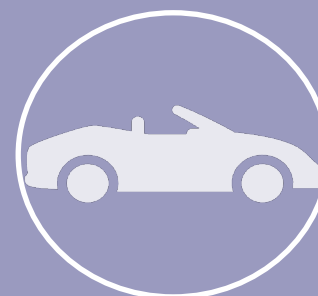
Placement

Illegal funds are first brought into the financial system.



Layering

This placement makes funds more liquid.



Integration

One could deposit cash into bank accounts or purchase assets with cash.



1.2 ML – TF : differences ?

Money Laundering

Illegal Proceeds
from initial offense

- Placement – process whereby funds are introduced into the financial system.
- Layering – process of disguising audit trail
- Integration – placing money back into economy as 'legitimate'.

Laundered Funds

Terrorist Financing

Illegal Proceeds

Licit Funds



Financing of Terrorist
Activities



Money Laundering, comprises 3 elements: primary offence, material element, intentional element.



1.3 Failing to comply with AML / CFT rules



For the individual

Prison

Fines

Discharged/Terminated

Professional reputation

Sanctions



For the company

Fines

Loss of banking license

Reputational risk

Sanctions



1.4 Entities in this scope?

Entities principally having a business in the financial sector and insurance are subject to AML/CFT regulations (non-exhaustive list)

- Credit institutions and professionals in the financial sector
- Payment institutions and electronic money institutions
- Insurance and insurance intermediaries
- Pension funds
- Investment funds, asset management companies
- Securitization undertakings
- Managers and advisors of undertakings for collective investment, investment companies in risk capital and pension funds
- Statutory auditors
- Accountants
- Notaries
- Lawyers
- Casinos



1.5 Initial/Predicate Offence

“**Initial Offense**” means the criminal activity underlying money laundering activities.

- Participation in organized criminal groups to racketeering;
- Terrorism including its financing;
- Trafficking in human beings;
- Sexual exploitation, including sexual exploitation of children;
- Drug and psychotropic substance trafficking;
- Illicit Arms trafficking;
- Illicit trafficking of stolen goods;
- Corruption;
- Fraud and embezzlement;
- Counterfeiting currency;
- Counterfeiting and parasitic copy of goods;
- Environmental Offense;
- Murder and serious body injuries;
- Theft;
- Kidnapping, deprivation of personal freedom and hostage taking;
- Smuggling;
- Breach of trust and misuse of company assets
- Extortion;
- Forgery;
- Piracy;
- **AGGRAVATED TAX FRAUD**
- **INSIDER DEALING AND MARKET ABUSE**

Primary Offenses can change between countries // EU initiative harmonization

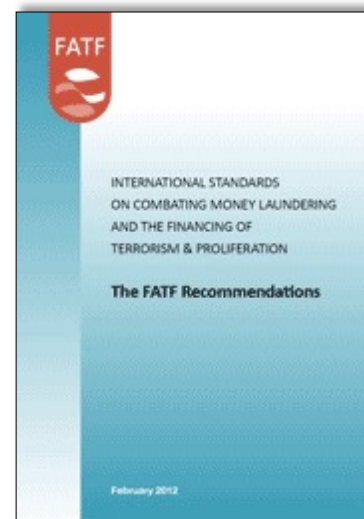


1.6 AML/CFT Main Obligations?

FATF recommendations related to the professional obligations :

<u>Number</u>	<u>Recommendation</u>
▪ 1	Risk-Based Approach *
▪ 10	Customer due diligence *
▪ 11	Record keeping
▪ 12	PEPs - Politically Exposed Persons *
▪ 15	New technologies
▪ 17	Reliance on third parties *
▪ 18	Internal controls, foreign branches and subsidiaries
▪ 19	Higher risk countries *
▪ 20	Reporting of suspicious transactions *

** The recommendation should be read with the respective interpretative notes*





Introduction to FATF-GAFI (1/2)

Creation

1989: creation of the Financial Action Task Force on Money Laundering (FATF/GAFI). An inter-governmental policy making body, based in Paris.

Objectives

- Sets international standards to combat money laundering and terrorist financing
- Assesses and monitors compliance with the FATF standards
- Conducts typology studies of money laundering and terrorist financing methods, trends and techniques
- Responds to new and emerging threats, such as proliferation financing of terrorism



Introduction to FATF-GAFI (2/2)

History

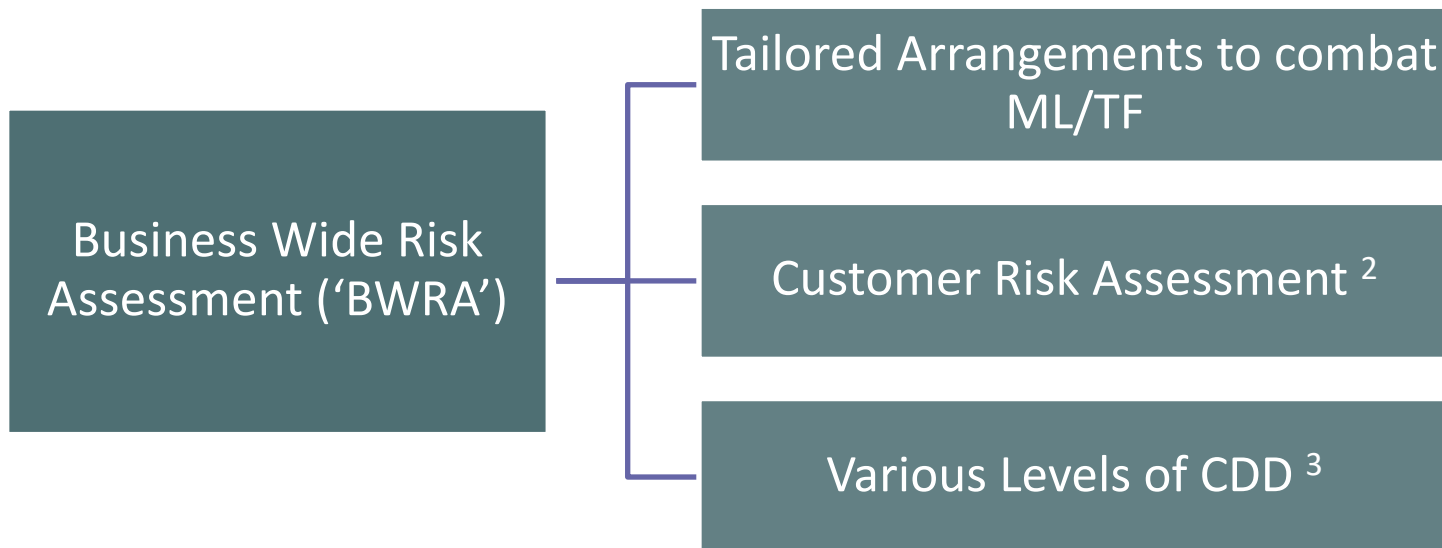
- 1990: 40 recommendations
- 2001: +7 special recommendations
- 2003: +2 special recommendations
- Revised in February 2012 to cover new threats such as the financing of weapons of mass destruction and to be clearer on transparency and tougher on corruption = a new set of 40 recommendations
- New priority areas such as tax crimes
- February 2013, FATF revised its risk assessment methodology



What does it mean for Professionals?

Carry-out a Business Wide Risk Assessment to identify ML/TF risks faced taking into account ¹:

- FATF/EU risk assessments
- National Competent Authority risk assessment (e.g. CSSF RA)



¹ Art. 4 CSSF Regulation 12-02 as amended, Art. 8.1&2 AMLD IV

² Art. 5 CSSF Regulation 12-02 as amended

³ Art. 4.(1) CSSF Regulation 12-02 as amended



RISK BASED APPROACH ('RBA')

What is Risk Based Approach ('RBA') ?

“Professionals are required to perform an analysis of the risks inherent to their business activities. They must set down in writing the findings of this analysis.”

Perform due diligence measures according to the identified risk level

- Risk assessment based on following risk factors:
 - Geography
 - Activity of the customer
 - Type of business relationship: services, products, transactions
 - Distribution channel
 - Assets
- Risk mitigation
 - Apply appropriate due diligence as per the risk level of the client
- Types of risk factors to be taken into consideration: customer, product, service, transaction, delivery channel, geographical area

Enhanced focus on the risk assessment and the associated risk based approach (4th and 5th AMLD and CSSF Circular 17/661)



1.7 Internal Organisation Framework

Person responsible

- ⇒ Appointed to be the point of contact for authorities

Policies and procedures

- ⇒ Available to staff
- ⇒ Define internal application of professional obligations

Control framework

- ⇒ Ensure efficiency of policies and procedures
- ⇒ All lines of defence

IT system

- ⇒ Ensure easy access to requested information
- ⇒ Ensure data accuracy/ record keeping

Training

- ⇒ Annual mandatory training for all staff

Recruitment/HR dimensions

- ⇒ Fit & proper (key functions)
- ⇒ New employee pack

1.9 Customer Due Diligence

Beginning of the business relationship

Identification

- Information/data on client

Verification

- Documentation/evidence of client data

Risk classification

- On a risk-based approach

Ultimate Beneficial Owner

- Natural person
- Capital ownership (>25%) and/or
- Power of decision and control

Name screening

- To detect politically exposed persons
- To detect international sanctions/frozen assets

Record keeping

- All data/documentation/controls
- At least 5 years after the end of the business relationship or the execution of the last transaction



ONGOING DUE DILIGENCE

Documentation to be kept up-to-date (regular review)

Transaction monitoring

Name screening



1.10 Law and Regulation on the register of beneficial owners

In this context, the BO has to be identified at the level of the umbrella.

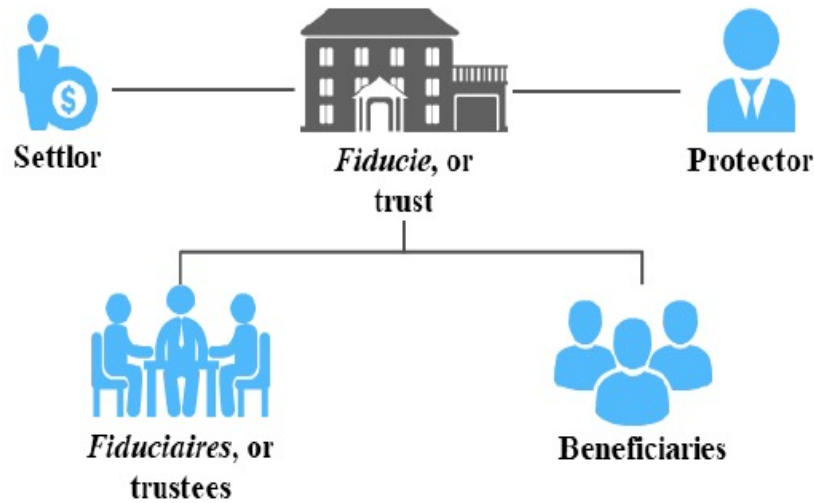
- If there is a direct or indirect investor above 25% - BO needs to be registered.
- If nominee (in an equivalent country) is above 25% but no underlying investor has over 25% - Nominee has to confirm that the underlying investors are below 25% (should be provided in accordance with the generic commitments obtained in AML comfort letters related to the identification and verification of clients and BO)
- If no investor (including Nominee) is above 25% - the BO is the senior managing official of the fund.

(* additional operational information are available in the Circulars LBR 19/01 and 19/02 issued by the Luxembourg Business Registers (“LBR”))



I. UBOS identification

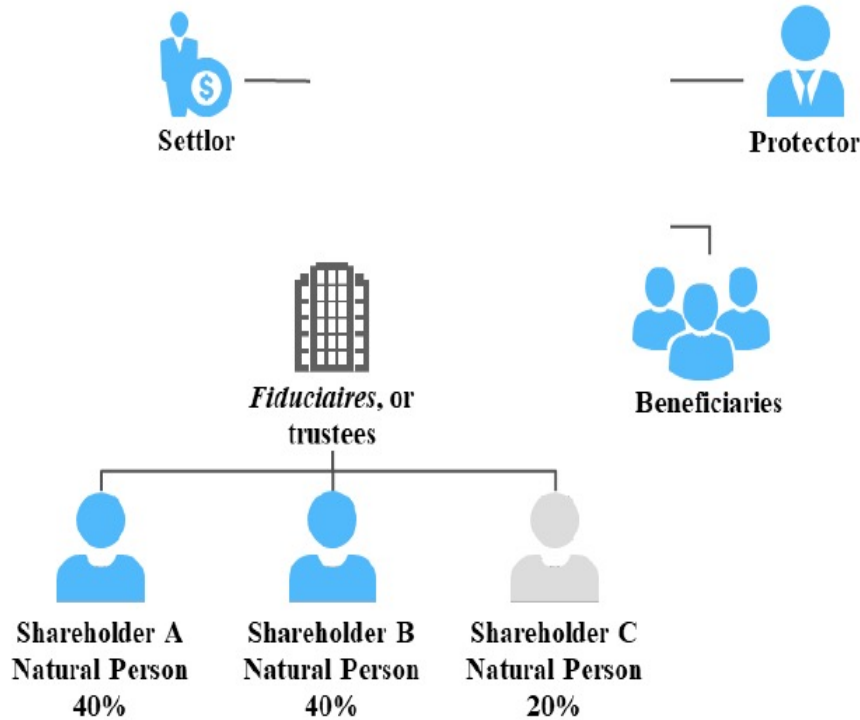
Figure 1: Trust Direct Ownership: All persons in blue have to be identified as UBOS





I. UBOS identification

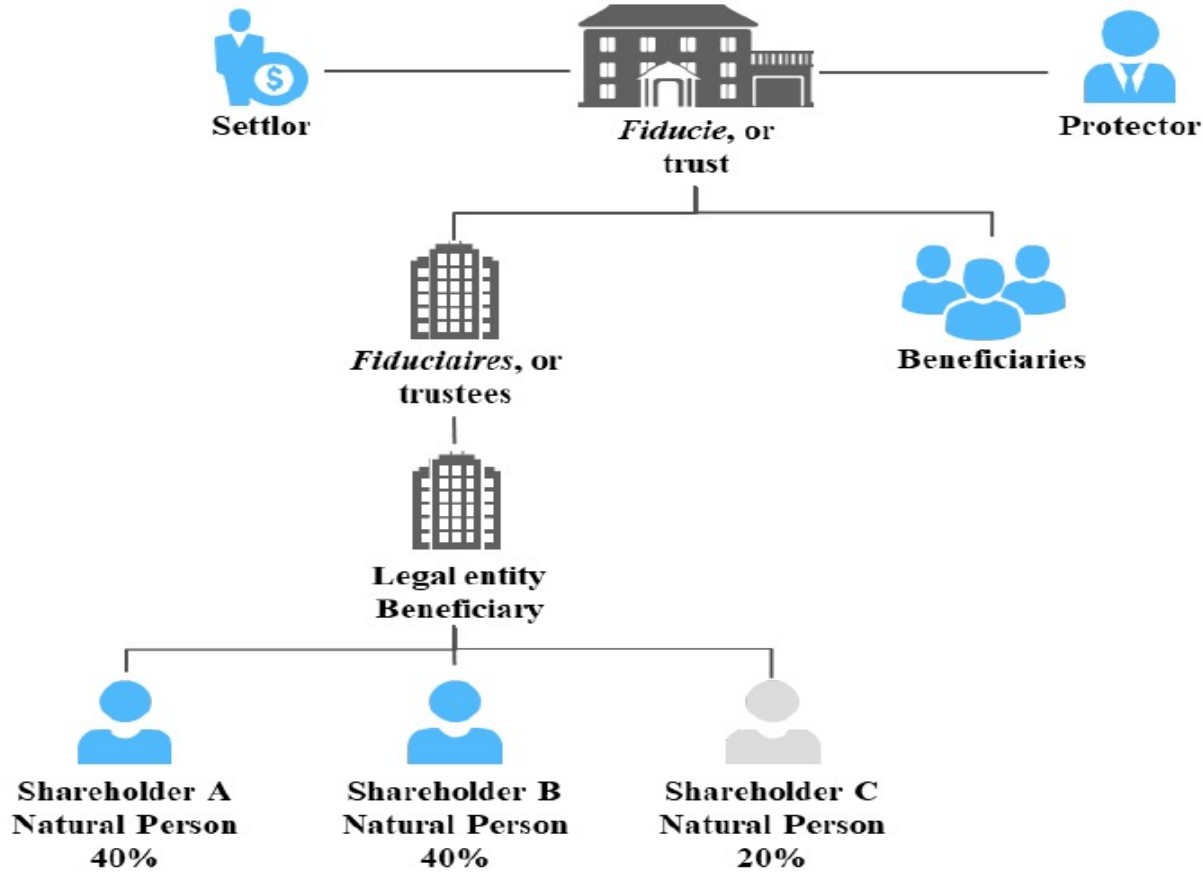
Figure 2: Trust: Indirect Ownership: All persons in blue have to be identified as UBOS





I. UBOS identification

Figure 3: Trust: Indirect Ownership





I. UBOS identification

Figure 4: Simple One Layer Ownership Structure

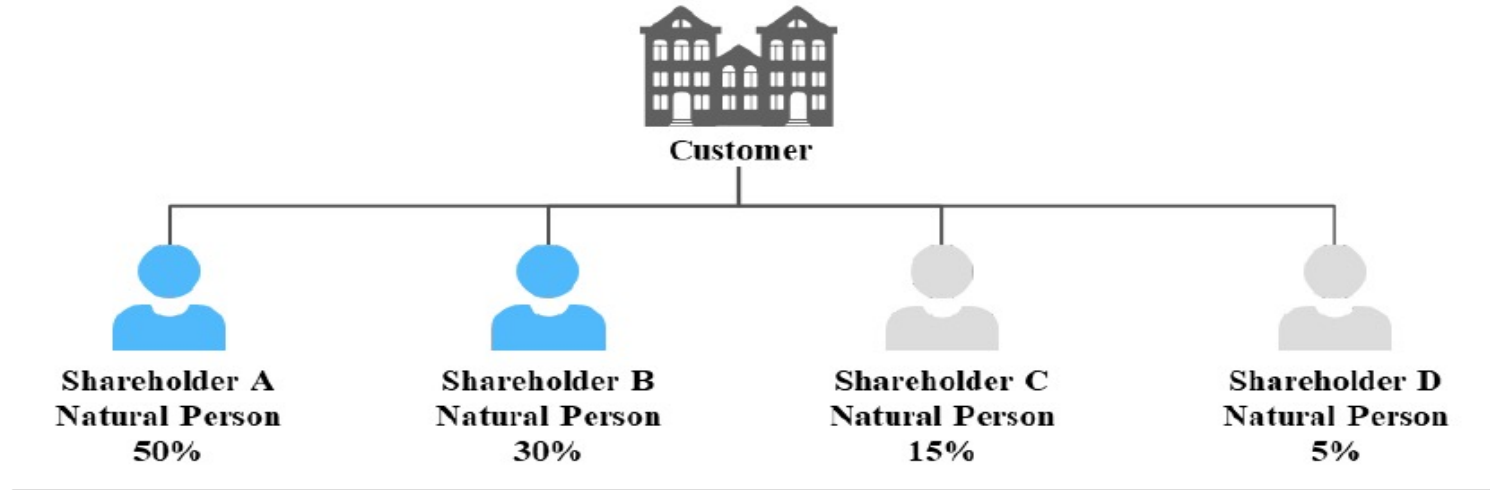


Table 4: Simple One Layer Ownership Structure³⁰

Shareholder	Type of shareholder	Type of ownership	Ownership	Beneficial owner
A	Natural	Direct	50%	✓
B	Natural	Direct	30%	✓
C	Natural	Direct	15%	x
D	Natural	Direct	5%	x



I. UBOS identification

Figure 5: Multiple Layer Ownership Structure

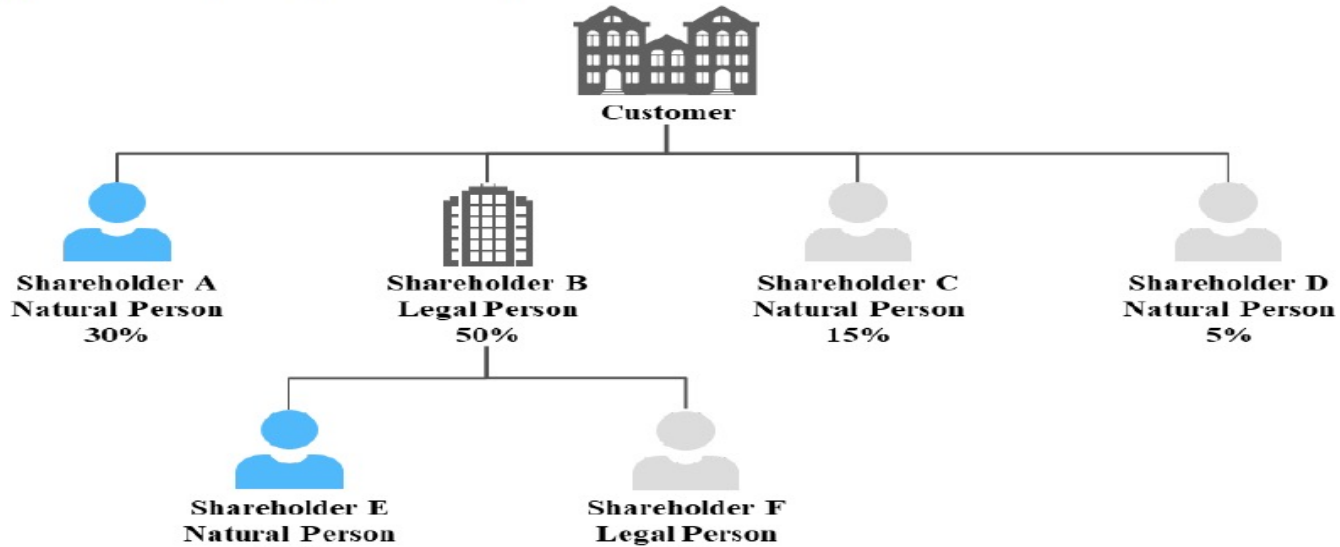


Table 5: Multiple Ownership Structure

Shareholder	Type of shareholder	Type of ownership	Ownership	Beneficial owner
A	Natural	Direct	30%	✓
B	Legal	Direct	50%	✗
C	Natural	Direct	15%	✗
D	Natural	Direct	5%	✗
E	Natural	Indirect	40%	✓
F	Natural	Indirect	10%	✗



I. UBOS identification

Figure 6: Cumulative Ownership

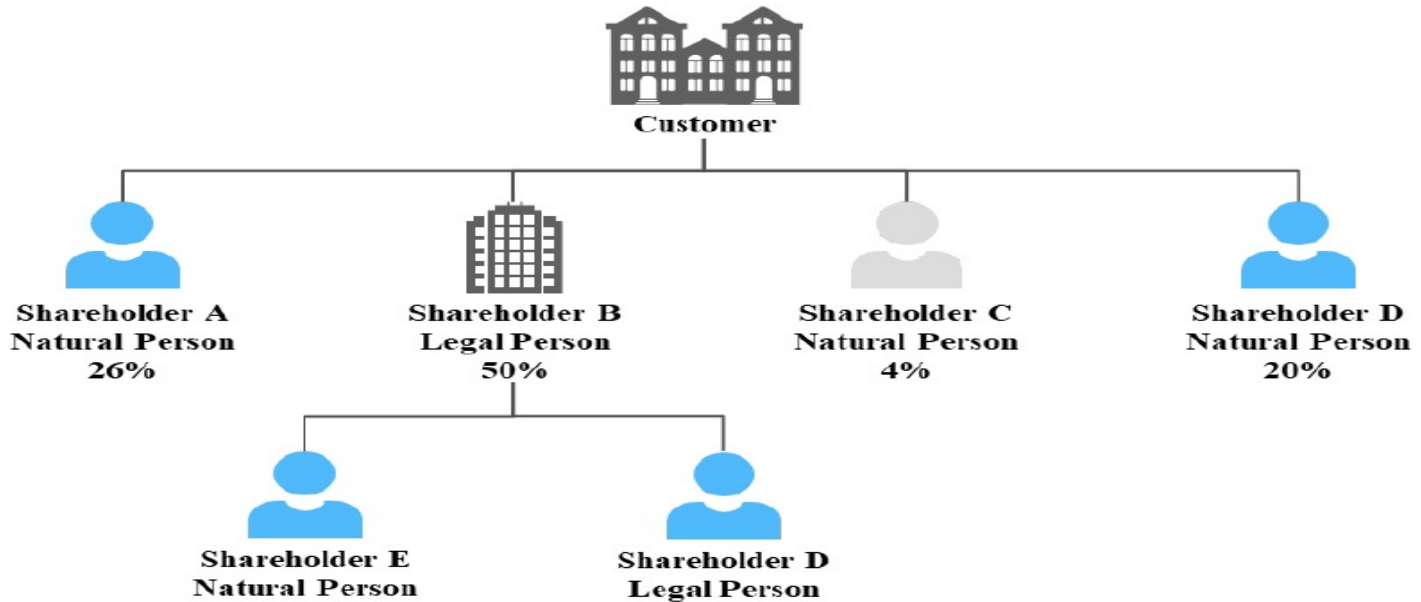


Table 6: Cumulative Ownership

Shareholder	Type of shareholder	Type of ownership	Ownership	Beneficial owner
A	Natural	Direct	26%	✓
B	Legal	Direct	50%	✗
C	Natural	Direct	4%	✗
D	Natural	Direct (cumulative)	30%	✓
E	Natural	Indirect	40%	✓



I. UBOS identification

Figure 7: In Concert Ownership

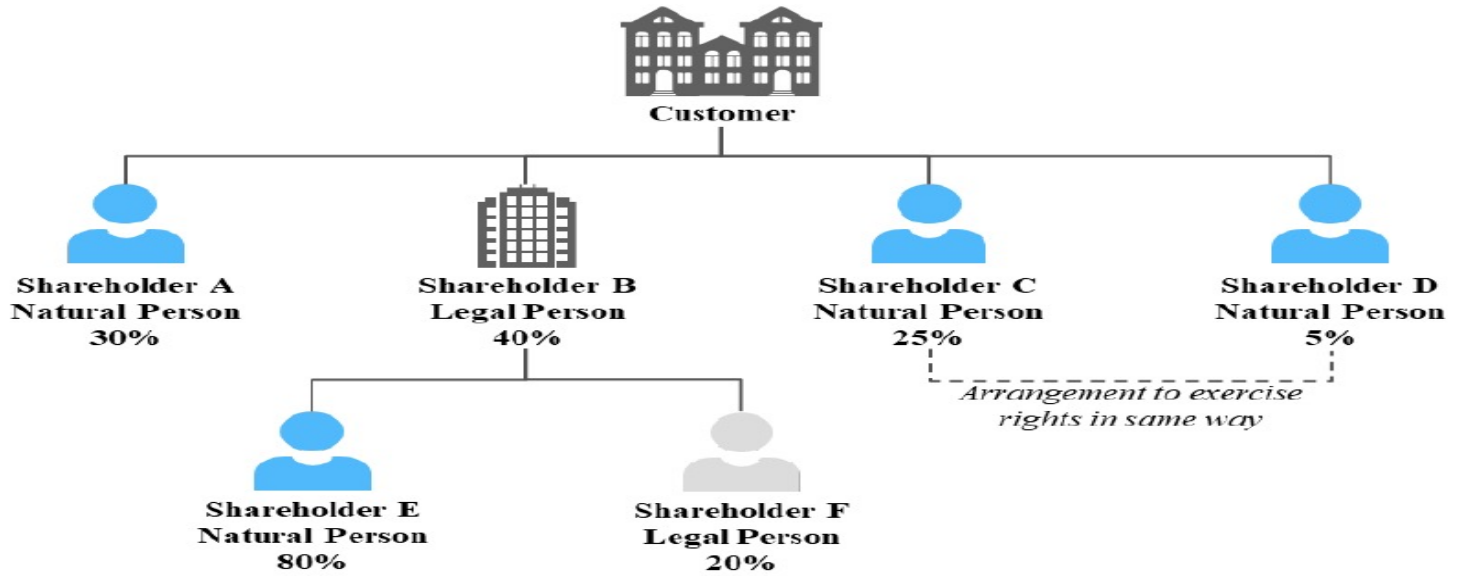


Table 7: In Concert Ownership

Shareholder	Type of shareholder	Type of ownership	Ownership	Beneficial Owner
A	Natural	Direct	30%	✓
B	Legal	Direct	40%	✗
C	Natural	Direct (joint)	30%	✓
D	Natural	Direct (joint)	30%	✓
E	Natural	Indirect	32%	✓
F	Natural	Indirect	8%	✗



I. UBOS identification

Figure 8: Decision Control over the Customer

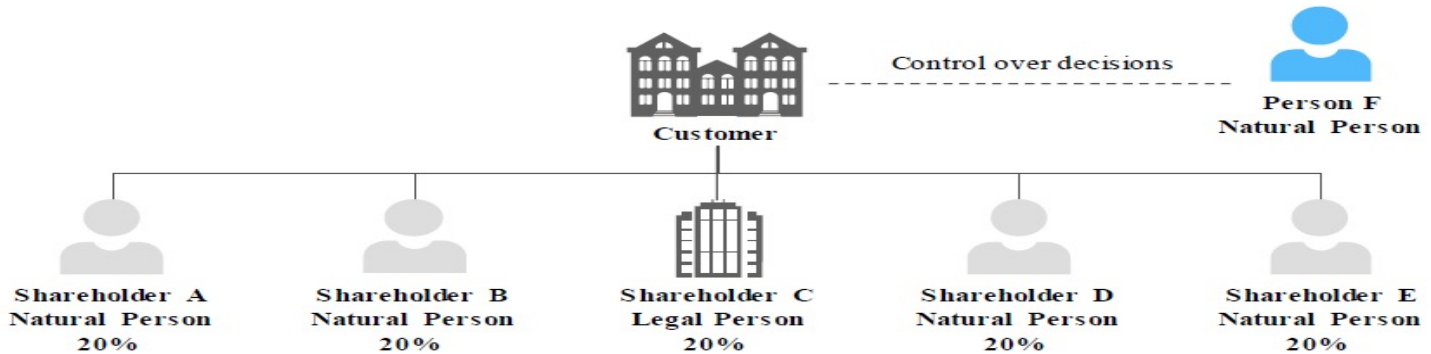


Table 8: Decision Control over the Customer

Shareholder	Type of shareholder	Type of ownership	Ownership	Beneficial owner
A	Natural	Direct	20%	✗
B	Natural	Direct	20%	✗
C	Legal	Direct	20%	✗
D	Natural	Direct	20%	✗
E	Natural	Direct	20%	✗
F	Natural	Decision control	0%	✓



I. UBOS identification

Figure 9: Majority Control

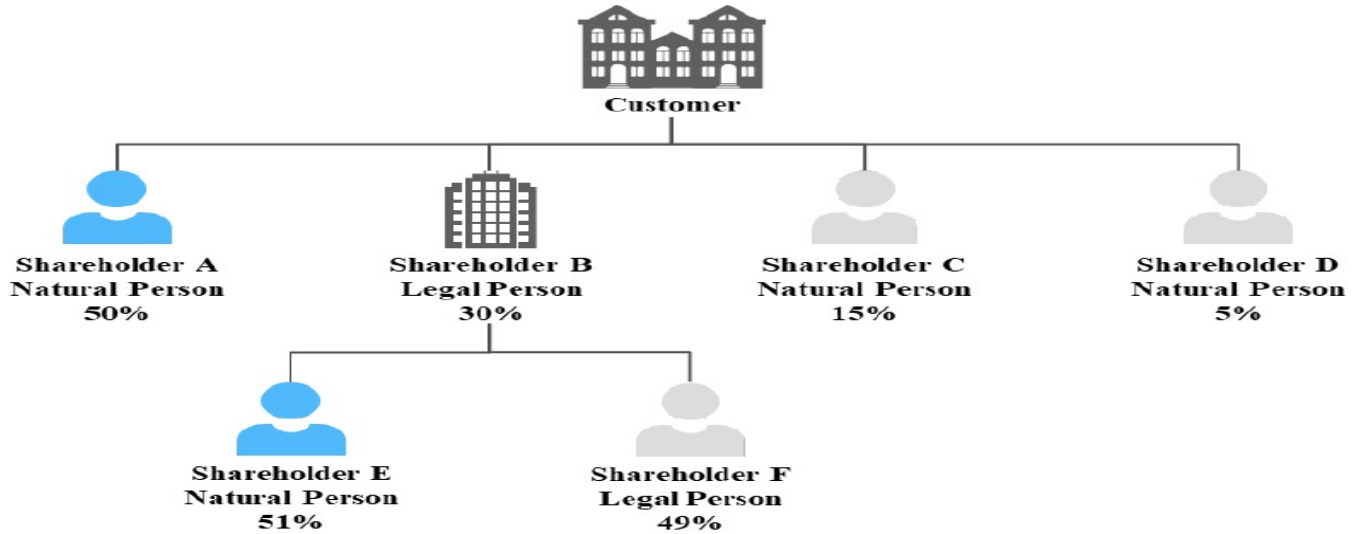


Table 9: Majority Control

Shareholder	Type of shareholder	Type of ownership	Ownership	Beneficial owner
A	Natural	Direct	50%	✓
B	Legal	Direct	30%	✗
C	Natural	Direct	15%	✗
D	Natural	Direct	5%	✗
E	Natural	Indirect (majority)	15.3%	✓
F	Legal	Indirect	14.7%	✗



I. UBOS identification

Figure 10: Decision Rights

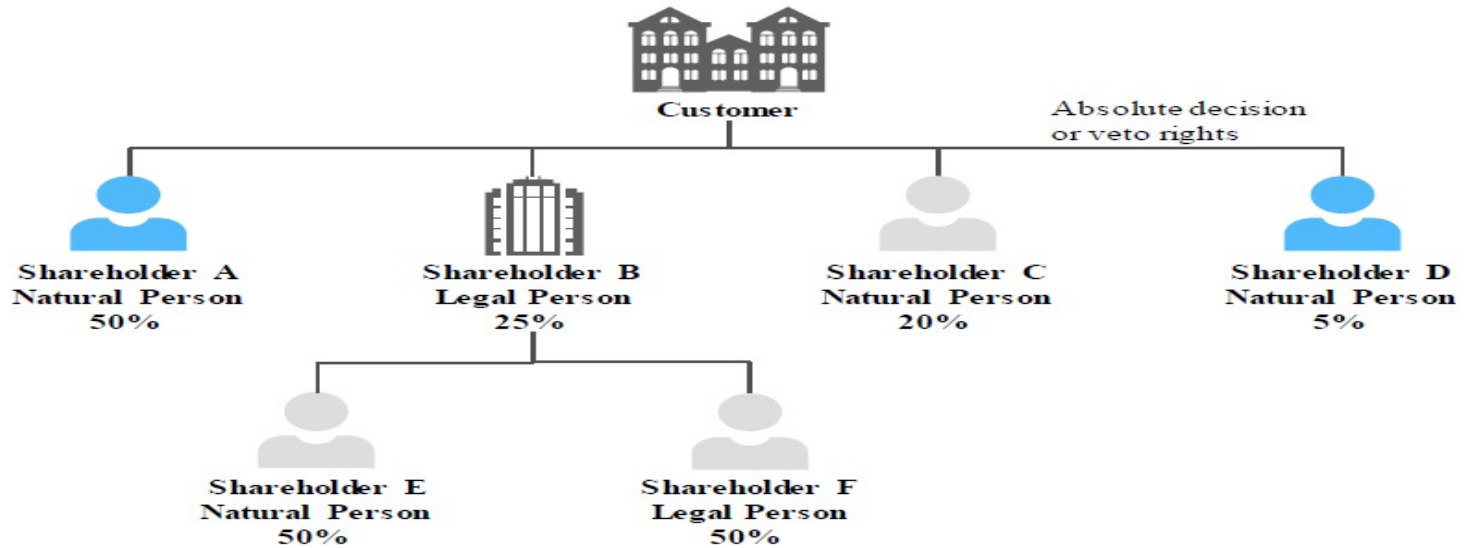


Table 10: Decision Rights

Shareholder	Type of shareholder	Type of ownership	Ownership	Beneficial owner
A	Natural	Direct	50%	✓
B	Legal	Direct	25%	✗
C	Natural	Direct	20%	✗
D	Natural	Decision rights	5%	✓
E	Natural	Indirect	12.50%	✗
F	Natural	Indirect	12.50%	✗



Figure 11 : Senior Managing Official

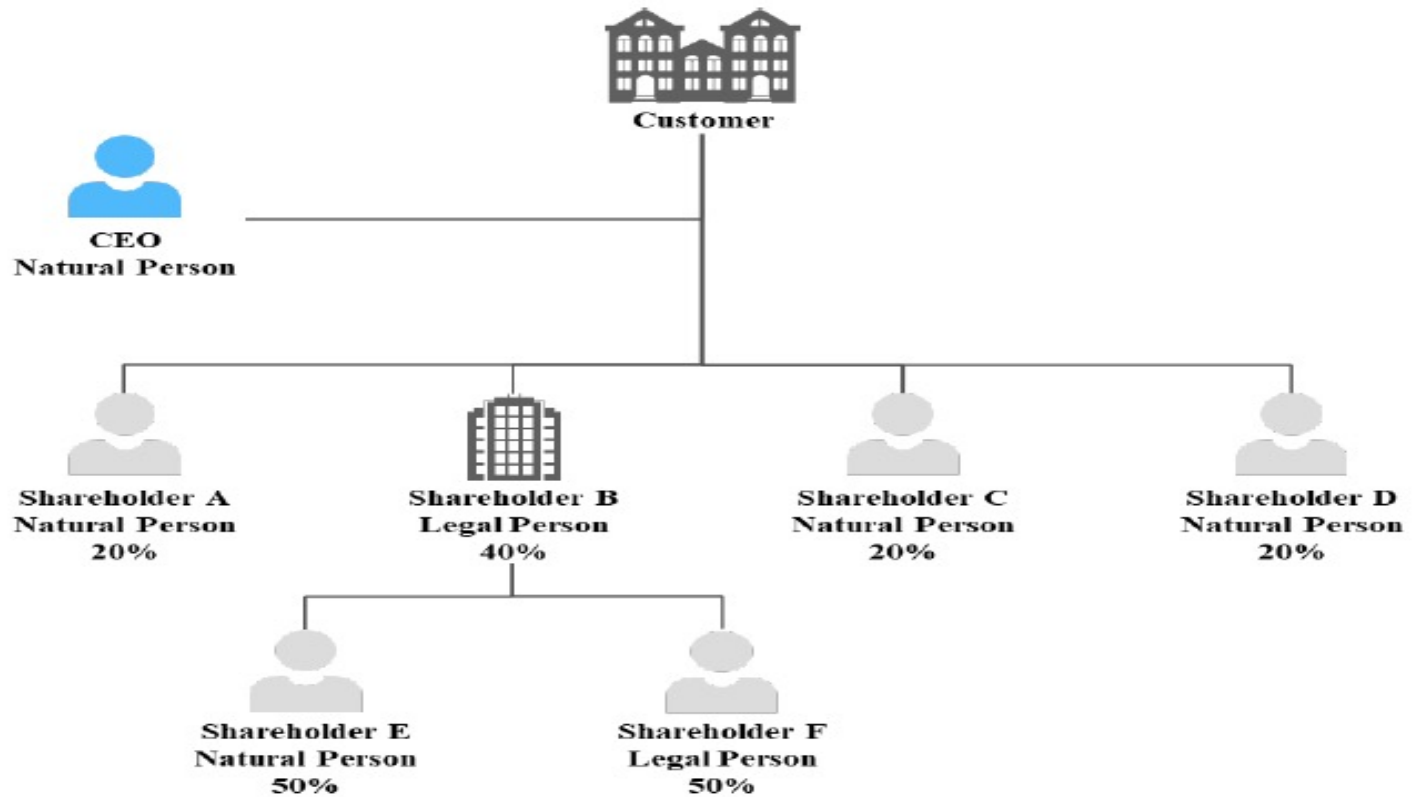
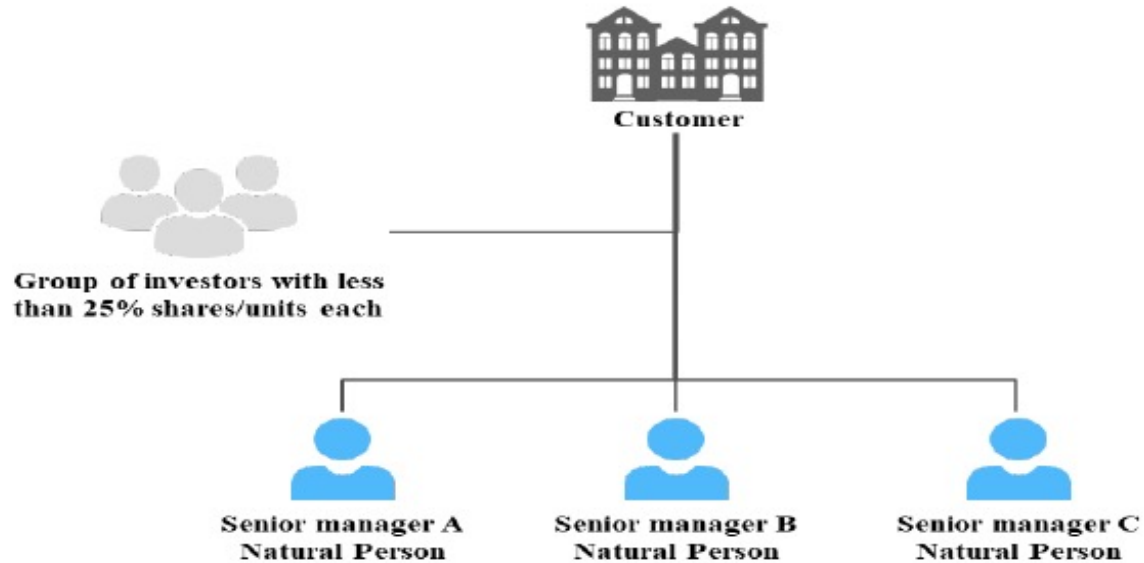




Figure 12: Senior Managing Official



In this example, the three senior managing officials should be identified as UBOs.



Figure 13: Example ASBL (1)

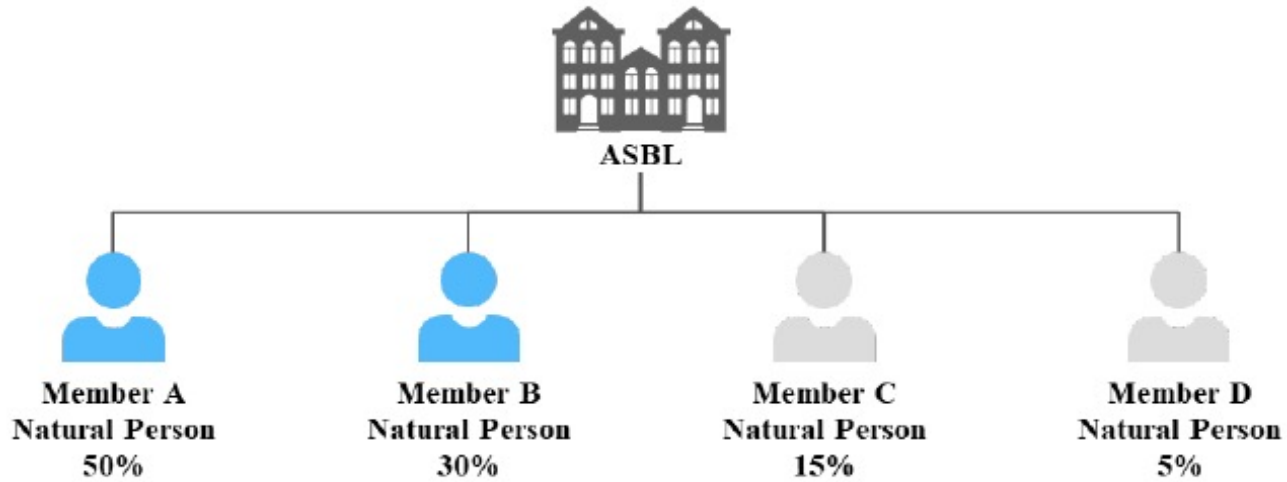


Table 13: Example ASBL (1)

Member	Voting rights	Beneficial owner
A	50%	✓
B	30%	✓
C	15%	✗
D	5%	✗



Figure 14: Example ASBL (2): The members of the board (*Conseil d'administration*) are to be considered as UBOs

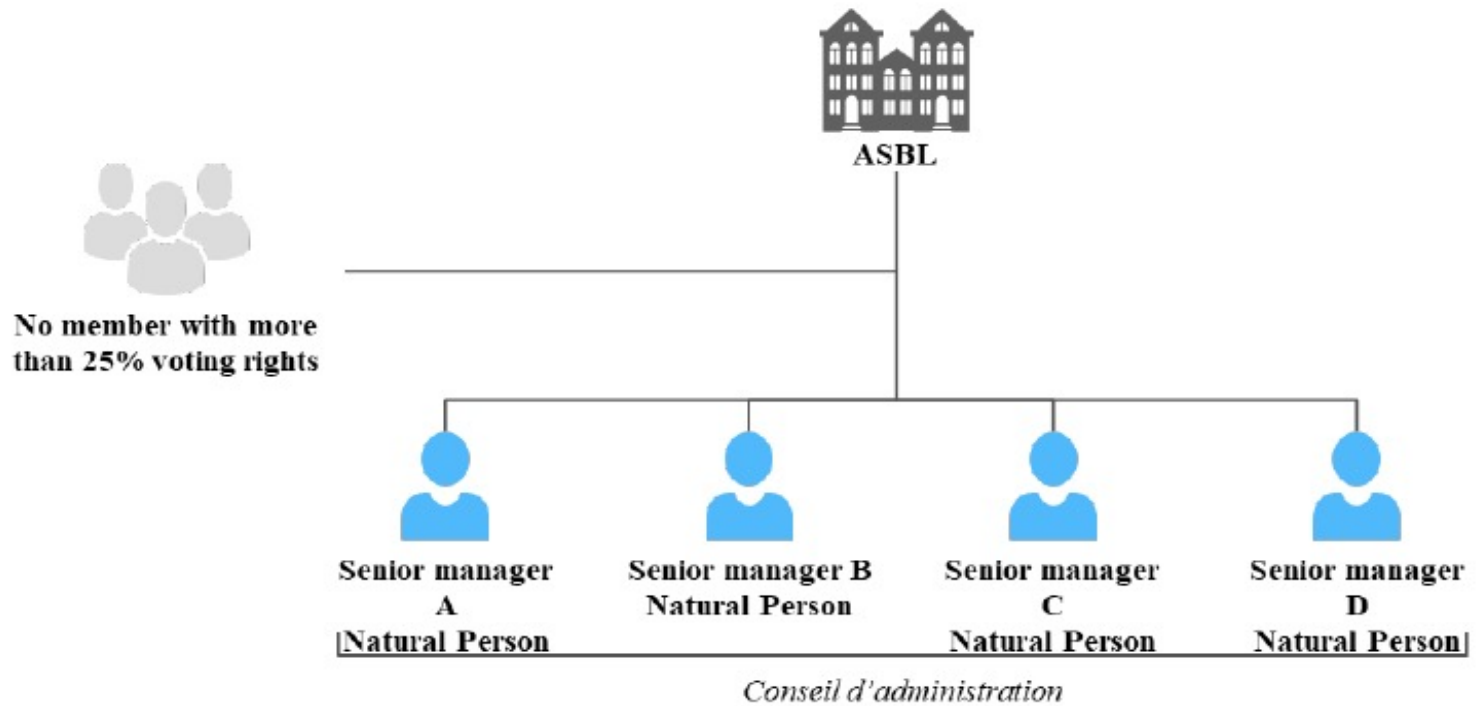
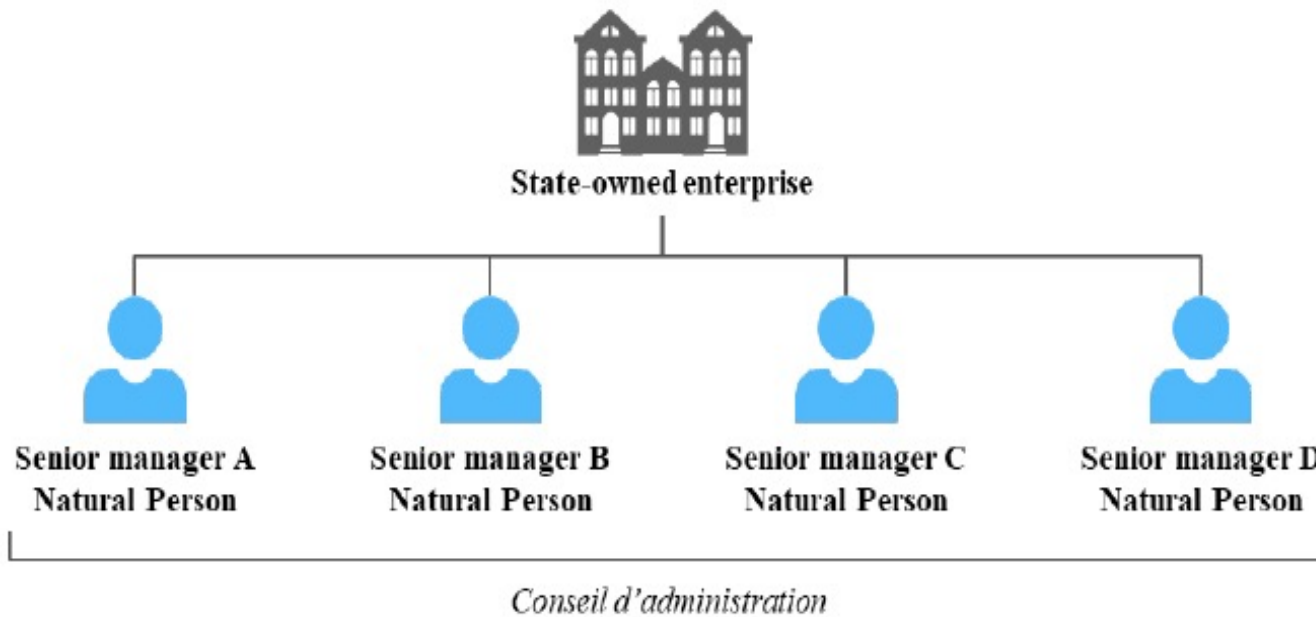




Figure 15: Public Administration: The members of the board (*Conseil d'administration*) are to be considered as UBOs





1.11 Political Exposed Persons - PEPs



Please observe these pictures and try to answer the following questions:

1- What PEP means ?

2- Who is a PEP (discuss your answer with participants)





5.4.5 Political Exposed Persons - PEPs





5.4.5 Political Exposed Persons – Definition (1/2)



Politically Exposed Persons (PEPs) are natural persons who are or have been (at least 12 months) entrusted with prominent public functions and family members or persons known to be close associates, of such persons.

- (a) Heads of state, heads of government, ministers and deputy or assistant ministers
- (b) Members of parliament or of similar legislative bodies
- (c) Members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances
- (d) Members of courts of auditors or of the boards or directorates of central banks
- (e) Ambassadors, chargés d'affaires and high-ranking officers in the armed forces
- (f) Members of the administrative, management or supervisory bodies of state owned enterprises
- (g) Important officials and members of the governing bodies of political parties
- (h) Directors, deputy directors and members of the board or equivalent function of an international organisation

Middle ranking or more junior officials do not fall in the scope.



Domestic PEPs are now in scope of the PEP definition



5.4.5 Political Exposed Persons – Definition (2/2)



Family Members refers to:

- (a) Spouse;
- (b) Any partner considered by national law as equivalent to the spouse;
- (c) Children and their spouses or partners;
- (d) Parents;
- (e) Brothers and sisters.



Persons known to be close associates refers to:

- (a) any natural person who is known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations with a PEP
- (b) any natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up de facto for the benefit of a PEP.



Customer Due Diligence Requirements

PEP Screening

- **When:** at inception and on a regular basis (no less than every six months - Art. 30 CSSF Regulation 12-02 as amended)
- **What:** All parties to a business relationship including UBO, minority shareholders/controlling persons, signatories, introducers, sponsors, senior management, beneficiaries of payments
- **How:** Automated system methodology (check 1/3 provider methodology)



THE FREQUENCY OF SCREENING SHOULD BE BASED ON A RISK ASSESSMENT AND DOCUMENTED



Customer Due Diligence Requirements (2/)



REMINDER: PEP High Risk Clients by default !

- Carry-out **Enhanced Due Diligence** including:
 - Obtaining the source of funds and the source of wealth
 - Scanning for adverse news → assess your reputational risk
 - Obtaining detailed evidence on nature and purpose of the business relationship
 - Additional proof where relevant: Identification, addresses, fiscal situation, type of activities ...

- Carry-out **Enhanced Ongoing Monitoring**: more frequent reviews of KYC documentation, lower monitoring thresholds, more frequent retrospective checks of transactions/activities, inflow/outflow controls



Customer Due Diligence Requirements (3/3)

Governance

- Business relationships must be signed off by authorised senior management
- Money Laundering Reporting Officer ('MLRO') maintains a list of all business relationships with a PEP status
- Board – Senior Management is regularly informed through MIs
- As a Board member, if you are a PEP or associated with a PEP as defined in law, you must disclose your status to the Chief Compliance Officer

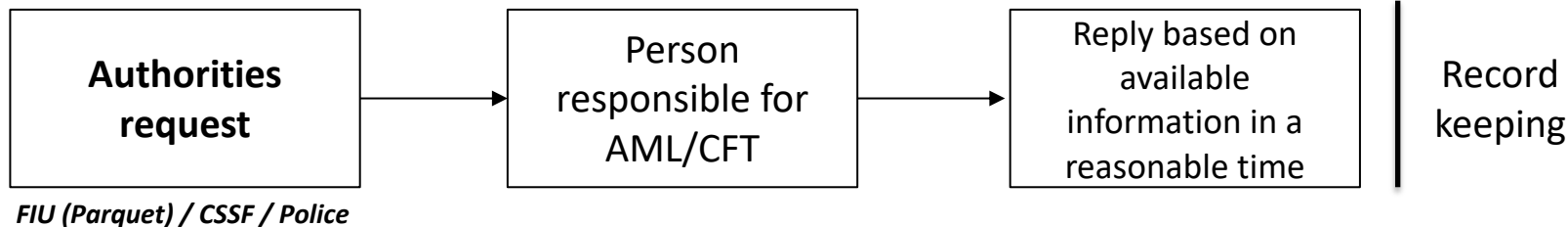


A dedicated policy should be adopted to document the process and ensure that all required regulatory obligations are complied with.

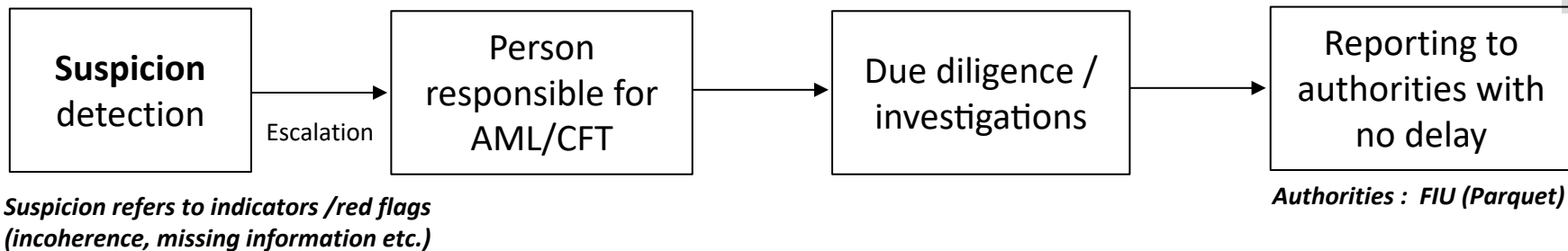


1.12 Cooperation with Authorities

Passive Cooperation



Active Cooperation



NO TIPPING-OFF : Prohibition to inform client or any third party
HOLD TRANSACTION : If transaction is in progress,
hold the execution of the transaction (not applicable for trade execution)



Cases studies



Case study #1

- Your client has an account with your bank from the last three years. The customer service department inform you (as MLRO) that the mailing details of this client has been returned to the bank over the last two months, even though there is still some activity on the account.
- Looking at the client profile, the client is a man, married and he has three children.
- Looking at the transactions, the only operations are:
 - Unemployment and government subsidy monthly inflows; and
 - Outflows such as cash withdrawals by using an ATM located in a neighbouring country.

Question : What is your view on this situation ?



Case study #2

- Two people come to your bank to open an account for each of them. One month later, each of them asks for a loan to buy a car.
- In order to provide some guarantee on these loans, they provide a copy of their payslip and working contract. The employer of both persons is a company based in Slovenia.
- As part of your due diligence controls, you cannot find the existence of such company and cannot reach anyone at the number and address provided for the employer.
- You call back your new clients who told you that the company has just been created but is not already registered by the public trade register website.
- However, during the next three months, the salary is still paid on a monthly basis on the client's accounts.

Question : What do you think about this situation and what do you do?



Case study #3

- You receive an internal report from the head of the cash desk explaining that one of your clients Mr. Zen (80 years old) has an account open in your bank for more than the last 20 years.
- He came to the bank together with a young man Mr. Joy and they have asked to withdraw € 50,000.
- The cashier has refused to give such an amount in cash because no valid explanation was provided. So Mr. Joy has requested to have those funds transferred to his personal bank account (account held at the same bank but opened two months before) and mentioned that Mr. Joy is indeed his grandson. The explanation given about the purpose of the transfer is the purchase of a car.
- He has asked to keep this transaction secret and to not mention it to Mr. Joy's stepmother. She is co-account holder and only one signature is required.
- The transfer is executed as requested. Mr. Joy also has an account open in your bank.
- One week later, Mr. Joy comes back (alone) to the bank and asks to withdraw € 10,000 in cash and to prepare the same cash amount to be withdrawn next week.

Question : What do you do and/or recommend?



Case study #4

- One of your clients receives payments on a monthly basis to his personal account that is deposited from various companies, which are not his employer.
- The team in charge of transactions monitoring finds out those companies are service providers in the same field of activity as that of his employer.

Question : What action do you take on this situation?



Case study #5

- A financial institution in Luxembourg has contacted the client manager of an Italian Bank in order to open a bank account for a new Italian public company to be incorporated. Ownership is held for 65% by a Middle East Bank quoted on the Qatari stock exchange and for 35% by a businessman who is a member of Qatar.

Questions:

On what basis would you accept or decline such a customer?

Is an Enhanced Due Diligence necessary in this case? Please provide details for your answer.



Case study #6

- Mr. Ben is CEO of the Zoo Group, with 14 branches worldwide.
- Mr. Ben has been Home Secretary in an unstable country.
- Mr. Yup is general manager of Win, a foreign company registered in a low tax jurisdiction.
- Company View is a branch of the group Zoo.
- Company Win has signed a sale agreement with Mr. Ben, to sell him a real estate property for €10 millions.
- In order to make the purchase, Mr. Ben has transferred €1 million on the notary account. The money has been transferred from the foreign account of the branch of the Zoo group.
- The day before the completion of the transaction, the sale is cancelled and Mr. Ben requests the money to be returned on an account belonging to him in a foreign country.

Question

How should the notary react?

Analyse this situation and point out the 'red flags'



Case study #7

- Several private customers obtain consumer loans, by using fake documents.
- The monies have been transferred to the account of jihadist family members.
- The money was withdrawn in cash and shipped to Turkey via a transfer operator.
- In Turkey, individuals mandated by the Islamic State are responsible for channelling the funds to the real beneficiaries
- Prepaid cards are bought in a foreign country via internet to pay the various stakeholders

Question : What red flags do you identify?

Discuss the possible controls that could / should be put in place.



Case study #8

- You are a Compliance Officer of a Bank.
- You receive a request from your regulator if you have some business relationship with a company named “Blacklist Corp”.

Questions

What actions will you take to proceed with the request?

What actions will you take if you found out that you have a business relationship with this company?

What actions will you take if you found out that you had a business relationship with this company 4 years ago?

Please explain in details the process you will follow.



Case study #9

- Several private customers obtain consumer loans, by using fake documents
- The monies have been transferred to the account of jihadist family members
- The money was withdrawn in cash and shipped to Turkey, via a transfer operator
- In Turkey, individuals mandated by the Islamic State are responsible for channeling the funds to the real beneficiaries
- Prepaid cards are bought in a foreign country via Internet to pay the various stakeholders
- **What red flags do you identify?**
- **Discuss the possible controls that could / should be put in place.**



2. Tax reporting overview FATCA / CRS



2.1 FATCA - FOREIGN ACCOUNT TAX COMPLIANCE ACT

- FATCA was enacted in the USA on March 2010, FATCA aimed to increase US tax revenues by tracing persons who are deemed tax liable. To this end, banks outside the US are required to provide information to the US tax authorities, the Internal Revenue Service (IRS), on the identity and accounts of customers who are liable to pay taxes in the US (so-called: 'FATCA US Persons').
- The US concluded an Inter Governmental Agreement (IGA) with many countries . This gives some relief to Banks and the reporting of clients that are FATCA US Persons.
- There are two IGA models:
 - IGA Model-1: Reporting to the local tax authority
 - IGA Model-2: Direct reporting to the US IRS.



2.2 FATCA : Main Obligations

- FATCA Review: Classification and documentation of existing client database.
- New client on-boarding: Additional documentation must be obtained to determine the FATCA Status of new clients. The FATCA status can be established through a self-declaration by the client (W8, W9, ...).
- Monitoring change of circumstances: Comprises keeping client FATCA-status in the books up to date with any changes in US elements.
- Reporting: Comprises designing and developing solutions for annual reporting of the assets of all FATCA US Persons to the local tax authorities.



2.3 FATCA : Scope and US Indicia

US indicia for identifying US tax liability

1. US citizen/resident (green card) or entity incorporated in the US
2. US birthplace
3. US address
- 4a. Only US telephone number
- 4b. US and foreign telephone number
5. Transfers to US accounts (standing instructions)
6. Power of Attorney granted to person with US address (for individual accounts)
7. Hold mail and in case of US address only



2.4 CRS – Common Reporting Standards

A fully reciprocal standard for automatic exchange of information between tax authorities of participating OECD jurisdictions

- Similar to FATCA
- Defines reporting rules & due diligence rules for Financial Institutions
- Requires the signing of a Competent Authority Agreement (CAA) by each participating jurisdiction
- To be translated into domestic law by jurisdictions that sign the CAA
- To detect and deter tax evasion through inter-governmental tax cooperation



2.5 CRS - Main Obligations

Account holder due diligence

- All account holders maintained by CRS Reporting FI must be linked to a tax residence.
- Account holders must be given a CRS classification and identified as “reportable” or “non reportable” account holders.

Legal entity classification

- Entities located in a CRS participating country must be classified and documented from a CRS perspective.
- Entities classified as Reporting Financial Institutions will have CRS obligations and will be solely responsible towards their local tax.

Reporting

- Identify which countries have signed an agreement with the FI’s country.
- Report to the local tax authority all accounts held by a Reportable Person on a yearly basis (obligation to inform clients).



2.6 CRS - Scope and Indicia

- Address in a CRS jurisdiction (mailing, PO box, residence, C/O)
- Phone number from a CRS jurisdiction
- Standing instructions to the benefit of an account maintained in a CRS jurisdiction
- Power of attorney granted to a person with a CRS jurisdiction address



2.7 FATCA/CRS Reporting

Reporting Deadline for FATCA/CRS is 30th June of each year

	FATCA	CRS
Name, address, TIN	✓	✓
Date and place of birth (individual only)	-	✓
Accounts numbers	✓	✓
Accounts value	✓	✓
Payments to the accounts (interests, dividends,...)	✓	✓
Gross proceeds on accounts	✓	✓



3. Predicate Offence: Market Abuse





3.1 What is "Market Abuse"?



- **Market abuse** occurs where investors are disadvantaged directly or indirectly by others who have:
 - Used information which is not publicly available
 - Disseminated false or misleading information
 - Distorted the price-setting mechanism of financial instruments

- EU member states prohibit:
 - Insider trading
 - Market manipulation



3.2 Market Abuse

- The Market Abuse Directive 2003/06/EC ("MAD"), adopted on 28 January 2003 by the European Council and the European Parliament introduced and implemented dissuasive measures and appropriate sanctions to fight illicit behaviour such as insider trading and market manipulation.
- Regulation (EU) No 596/2014 of the European Parliament and the Council of 16 April 2014 on market abuse (market abuse regulation) came into force in July 2016
- Some behaviours are prohibited (Insider Trading, Market Manipulation)
- Some specific obligations apply to:
 - Issuers of listed financial instruments
 - Their management and relatives
 - Persons issuing public recommendations (market analysts)
 - Financial institutions (banks, financial service providers)
- Dissuasive sanctions have been defined



3.3 Insider Trading (1/4)

There are two types of “insiders”

- Primary insiders
 - Shareholders
 - Management
 - Employees and external contributors in the course of their professional activities (external auditor, lawyers, advisors...)
 - Authors of criminal activities
- Secondary insiders
 - All others who obtain information (from primary insiders) that they know, or should know, to be inside information
- The applicable sanction depends on qualification of the type of insider.



3.3 Insider Trading (2/4)

- **Insider trading**
 - => is the act of carrying out transactions on financial instruments listed on a regulated market (e.g., a stock exchange), using internal/privileged information (even if the transactions take place outside of a regulated market)
 - e.g., a person has information on a takeover bid that is not yet available to the public and uses it, although he knows/should have known it was inside information
- **Inside/privileged information is information that meets four criteria:**
 - It is of a sufficiently precise nature
 - It has not (yet) been made public
 - It relates to one or several issuers of financial instruments or one or several financial instruments
 - It is likely to have a significant impact on the market price of those financial instruments, if it were made public



3.3 Insider Trading (3/4)

- **What is meant by public information?**
 - Information that has already been publicly released
 - Or, that is already known by a large section of the public
- **What can be done to avoid problems?**
 - Print and save the dated public information on which the investment decision has been based
- **What is meant by information of a precise nature?**
 - If it refers to a set of circumstances or to an event that has arisen or is likely to arise **and**
 - If it is possible to conclude from the event/circumstances to an effect on the price of a financial instrument



3.6 Insider Trading (4/4)

- **It is forbidden to use insider information for**
- **Sale or purchase for an own account** or for the account of somebody else, directly or indirectly, e.g., by buying securities in order to realise a gain or selling them in order to minimize a loss
- **Communicating/disclosing inside information** to a non-authorized party (unless necessary in a normal professional context)
- **Recommending a third party** to buy or sell a financial instrument, on the basis of inside information (that you don't disclose)



3.7 Market Manipulation

This means:

- Carrying out transactions
- Giving instructions or giving out false or misleading information (e.g., about a company's good or bad financial situation)
- Where a person knowingly tries to mislead other investors or influence the price of a financial instrument



3.8 Obligations for Financial Institutions

- Create and keep updated a list of insiders within an issuer company (permanent or occasional)
- Prevention: code of conduct (e.g. the international code of conduct of the Financial Markets Association)
- Training of employees and procedural implementation (detection programme)
- Flag clients & employees who are at risk and need closer monitoring of their transactions in relation to their sensitive positions (including secondary insiders)
- Monitoring of personal transactions and client transactions
- Suspicious transaction reporting



3.9 The role of the Compliance Officer with regard to EMIR

Depending on the financial institution, the role of compliance may be limited or extended. At the very least the compliance function must ensure that:

- the 3 duties (clearing, reporting, mitigation of risk) are taken care of
- responsible staff members were appointed to be in charge of each of these duties
- an escalation procedure is implemented in order to inform senior management and compliance



3.10 Market Abuse Criminal Sanctions

	Natural Person		Legal Person
	Prison	Fine	Fine
Insider dealing * x 10 times the profit	3 months to 2 years	€ 251.- to € 5.000.000.-	€ 500.- to € 15.000.000.-
Market manipulation			
Unlawful disclosure of inside info	8 days to 2 years	€ 251.- to € 500.000.-	€ 500.- to € 1.500.000.-



- A consultant specialised in mergers and acquisitions is currently assisting company ABC, which is listed on Euronext, in preparing a takeover of company XYZ, which is listed on the German Stock Exchange
 - When working late at the office, the cleaning woman/man overhears the consultant discussing the takeover on the telephone
 - The next day she/he suggests to her/his son to purchase shares of XYZ
- ***Who would be in trouble in this case?***



- You invited several friends to your house for a drink. One of your friends, a corporate lawyer, calls to tell you that he/she cannot attend your drink, because he/she is working on a big deal, involving Big Holding Company and Major Bank.
 - Specifically, he/she is preparing a meeting between the CEOs of both companies.
 - You are familiar with both Big Holding and Major Bank, because their shares are on the recommended list of your company.
- ***How would you react to the phone call from your friend?***



- Your client is a financial analyst, he works for a well-known London stock broker.
 - He (she) seems to have a very good “eye” for picking out stocks that go up
 - As Compliance Officer, what is your approach?
- ***How would you react to the phone call from your friend?***

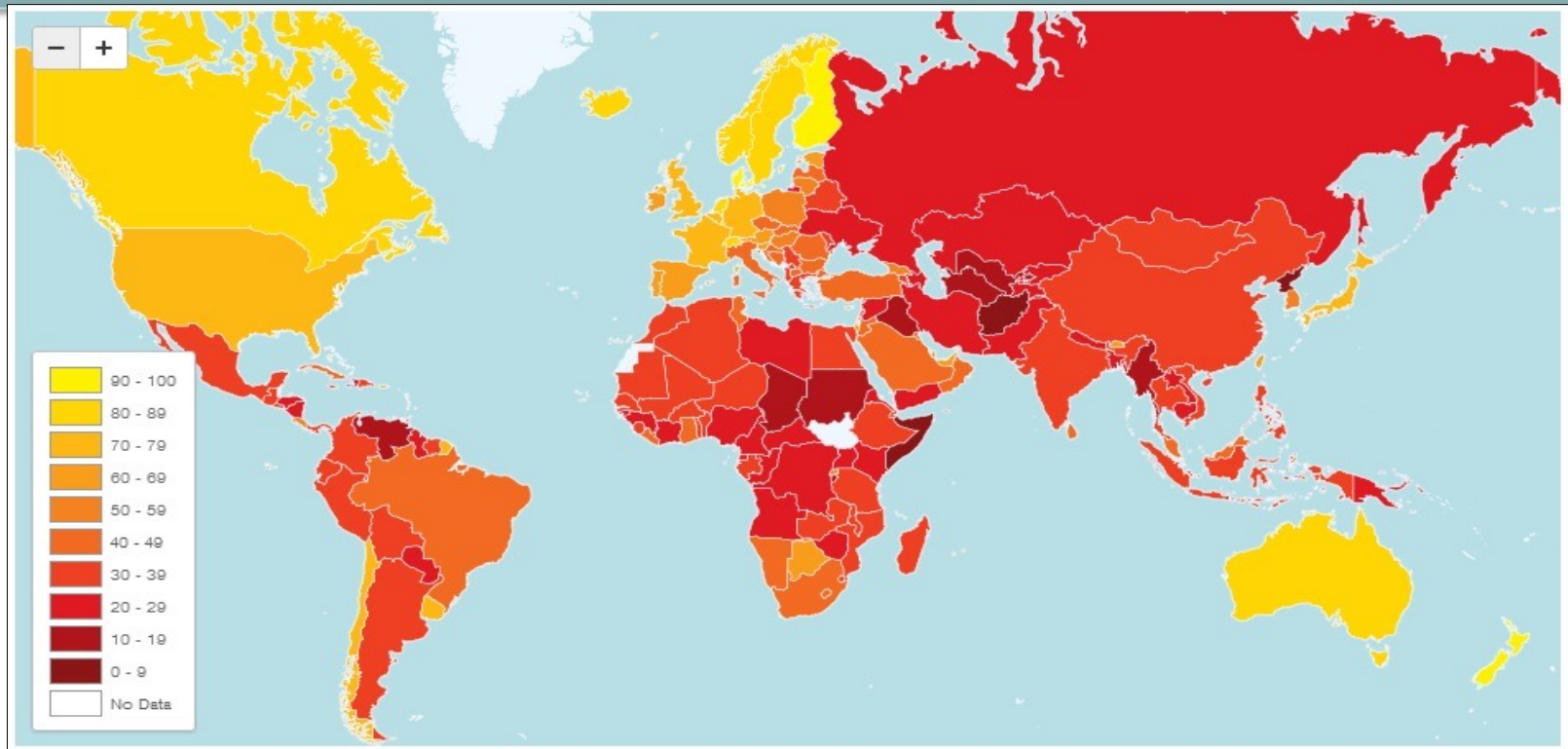


- You are the Compliance Officer of a listed company
- This morning, when you arrive at work, you receive an e-mail from one of your friends, asking you if it is true that your company is about to announce the sale of one of its core activities?
- There are rumours circulating on the internet...

➤ ***How do you react?***



Identifying High Risk countries is essential for an effective Compliance program





4. International Sanctions





4.1 International Financial Sanctions Overview

Definition



Sanctions or **restrictive measures** are actions taken by a country or several countries (unilateral/multilateral) against a targeted country, group, or individual, as a way of conducting standard behaviour (commercial or diplomatic). Economic sanctions may include various forms of trade barriers, tariffs, and restrictions on financial transactions.

Objectives

Political, Commercial, National Security, Inadequate international regulatory conduct



4.2 Differences between Embargo and Sanctions



An Embargo represents a complete ban on all commercial activity between two nations;

Sanctions are more limited in scope and prohibit trade in certain types of goods, sectors or transactions with particular individuals and entities.



4.3 Sanctions Requirement Challenges

The recent expansion and specialization of the international financial sanctions programs leads financial institutions to face growing challenges :

- EU sanctions are subject to national implementation of each member local regulator. In addition, each EU member can implement its own local list or local restrictive measures.
- Extraterritorial application of sanctions :
 - Sanctions apply globally to EU nationals; each EU member has enforcement authority of the EU sanctions programs
 - Sanctions apply to US persons (US citizens, US permanent resident, person located in the US), US entities and to USD denominated transaction wherever in the world



4.4 What is the SDN List?



SDNs : Individuals and companies, such as terrorists and narcotics traffickers listed by OFAC, are called "Specially Designated Nationals" or SDNs.

US individuals and entities can not do business with list members. It's a dynamic list, names are added and deleted at any time.

Penalties for non-compliance :

- Corporate and personal fines up to USD \$ 1 million and 12 years imprisonment;
- Confiscation of funds or other assets involved in the violation.



4.5 Sanctions Legal Basis

EU/Local regulation legal basis

- Articles 21 and 29 of the treaty of the EU and article 215 of the Treaty on the functioning of the EU
- National authorities of each EU member state are responsible for the implementation and enforcement of the EU sanctions programs
- Local regulations exist

US regulation legal basis

- Congressional authorization for the Executive branch to create sanctions programs under certain conditions.
- Executive orders (issued by the president of the US)
- Implementation and regulation by US administration, law enforcement agencies: US Treasury OFAC, US departments of Commerce and state



4.6 Sanctions Types

Sanctions include asset freeze and/or financial restriction or economic prohibitions, controls, can target individuals, entities, activities or a government.

- **Comprehensive sanctions programs:** sanction regime that targets the government of a country and prohibit a wide range of commercial activities and trade restrictions
- **Regime based sanctions programs:** sanction regime implementing limited trade restrictions or embargos and financing prohibition to a country
- **List /activity based sanctions programs :** sanctioning very specific activity (drug trafficking, terrorism, cybercrime.....) or including designations on list-based sanctions

Different types of entities concerned



Countries /
Régions



Goods



Criminal
Organizations



Physical listed
people



Business Activities,
Corporate



Vessels, shipping,
...





- COMPLIANCE, GENESIS & KEY PRINCIPLES
- COMPLIANCE FUNCTION FUNDAMENTALS
- FINANCIAL CRIME FRAMEWORK
- MIFID OVERVIEW**
- DATA PROTECTION

MIFID II OVERVIEW



Agenda

- 1. Introduction**
- 2. MiFID II Client Services**
- 3. MiFID II Governance & Supervision**
- 4. Conclusion**



1. Introduction





1.1 MiFID Introduction (1/2)



Following the turbulent years in the **financial markets during the 1990s**, EU legislators realised that a regulatory framework was necessary to provide and adequate investor protection framework

In 2007 MiFID I came into force and was the first major EU effort to put in place a comprehensive regulatory framework for financial markets.

In 2018, MiFID II is built on MiFID I – **you cannot be compliant under MiFID II if you are not fully compliant under MiFID**



1.1 MiFID Introduction(2/2)

- Formalised a series of concepts already deeply embedded in the financial industry, mainly on the banking side:
 - Client testing, now through formal suitability and appropriateness tests
 - Client risk profiling
 - Best execution
 - Governance set-up (compliance, audit, risks)
- Full transparency efforts in regard of equity trading by introducing new trading platforms (multi-lateral trading facilities – MTFs) as well as accompanying transparency obligations
- Introduced new concepts, including:
 - Inducements
 - Complex products



1.2 Was MiFID I a Success?



MiFID I brought EU financial markets on to a **single floor** (regulatory regime)

New **trading platforms** have emerged (e.g., 150 MTFs) and increased equity trading transparency

Customer protection has significantly increased, notably through more relevant information provided to the client, client profiling and client testing



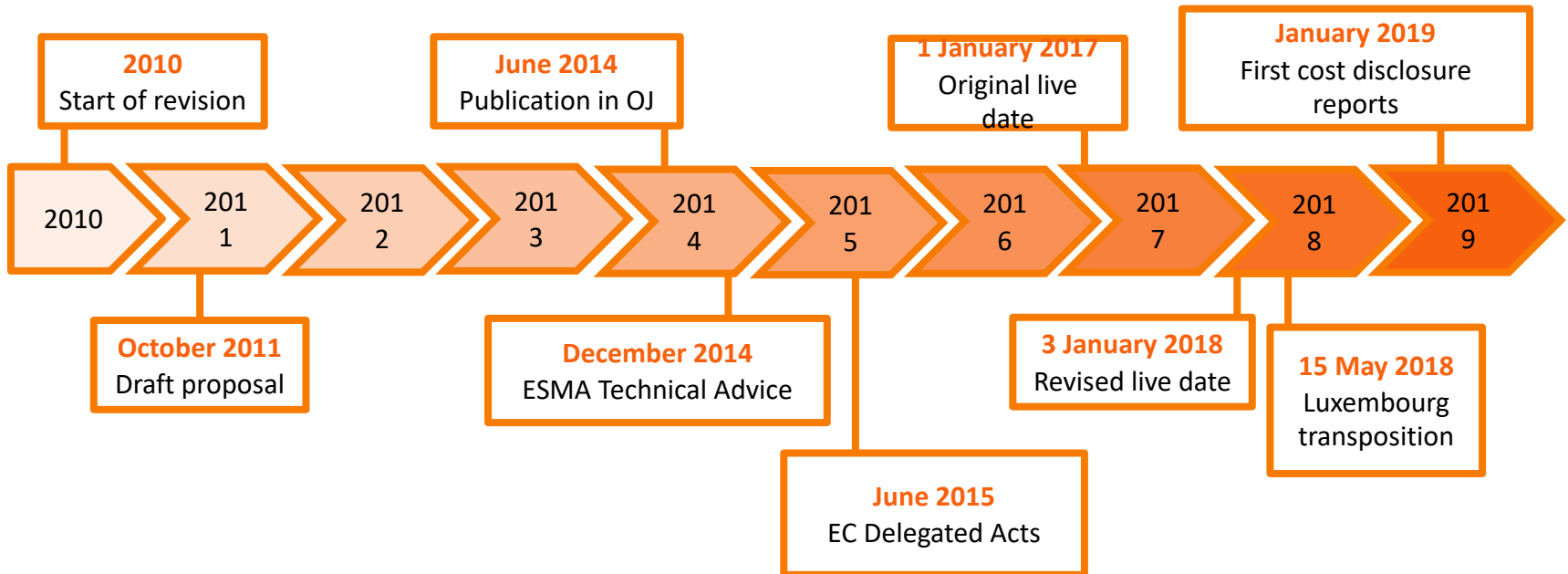
State of compliance under the MiFID I framework is still not unified (lack of regulatory guidance as well as local discrepancies)

New trading platforms fueled dark trading, high-frequency trading and algorithmic trading – thereby **limiting trading transparency**

Some rules were implemented as **policies** only



1.3 MiFID II sees the light of the day

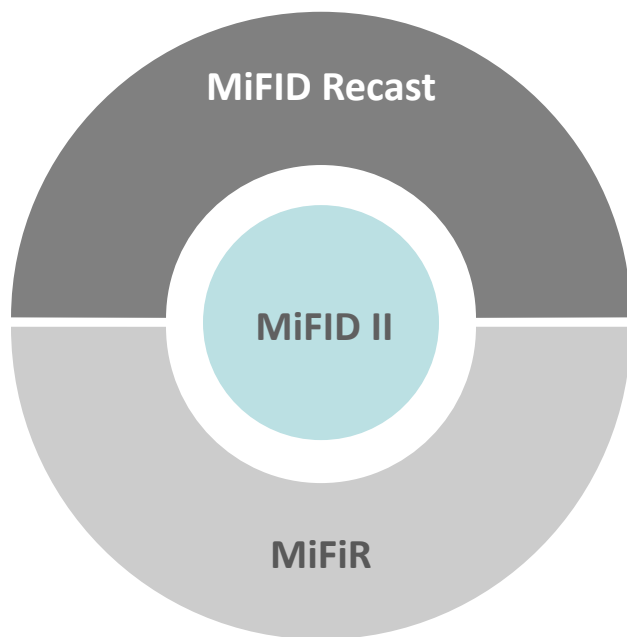


Until now > 7500 pages of technical standards and documents



1.4 The MiFID II Package

- 2 texts, 220 pages (level 1): a directive and a regulation
- 7,500+ pages when considering ESMA publications

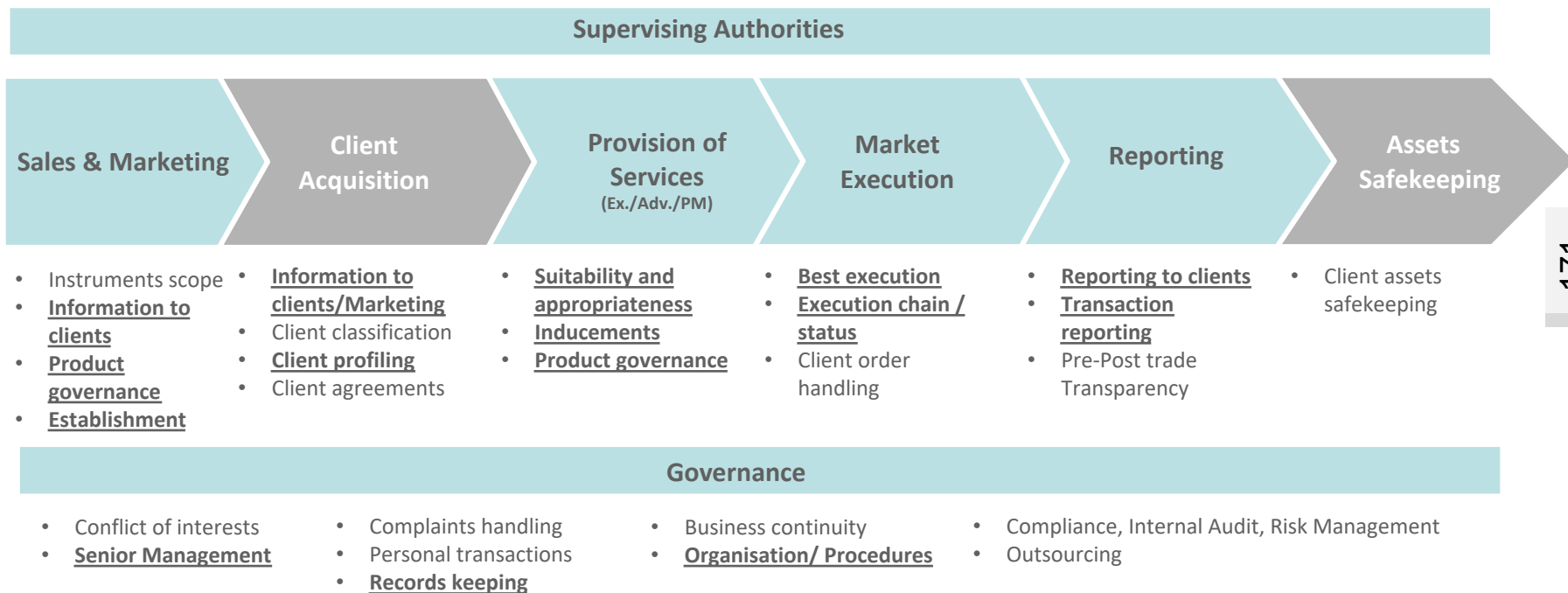


- Recast of Markets in Financial Instruments Directive (MiFID)
 - *General-supported by implementing standards on levels 2 and 3*
 - *Focus- on investor protection (conduct of business rules and suitability/appropriateness testing as well as best execution), but not only:*
 - *Management responsibility*
 - *Inducements*
 - *Product approval*
 - *Transposed into national law*
- New Markets in Financial Instruments Regulation (MiFIR)
 - *Focus on all matters where full harmonisation is critical, market organisation and transparency:*
 - *Transaction reporting*
 - *Pre- and post-trade transparency requirements*
 - *High degree of technicality, complemented by RTS*
 - *Part of a wider “rule book” with other regulations*
 - *Includes aspects of supervision*
 - *Direct effect without any need for local implementation*



1.5 MiFID II Impact on financial services firms

- SCOPE, MEANS, RESPONSIBILITIES



More than a fin -tuning exercise, requiring firms to proceed with a full gap analysis against MiFID I to identify where updates and reviews are required (e.g. complex products lists, best execution, client testing, information and disclosures)



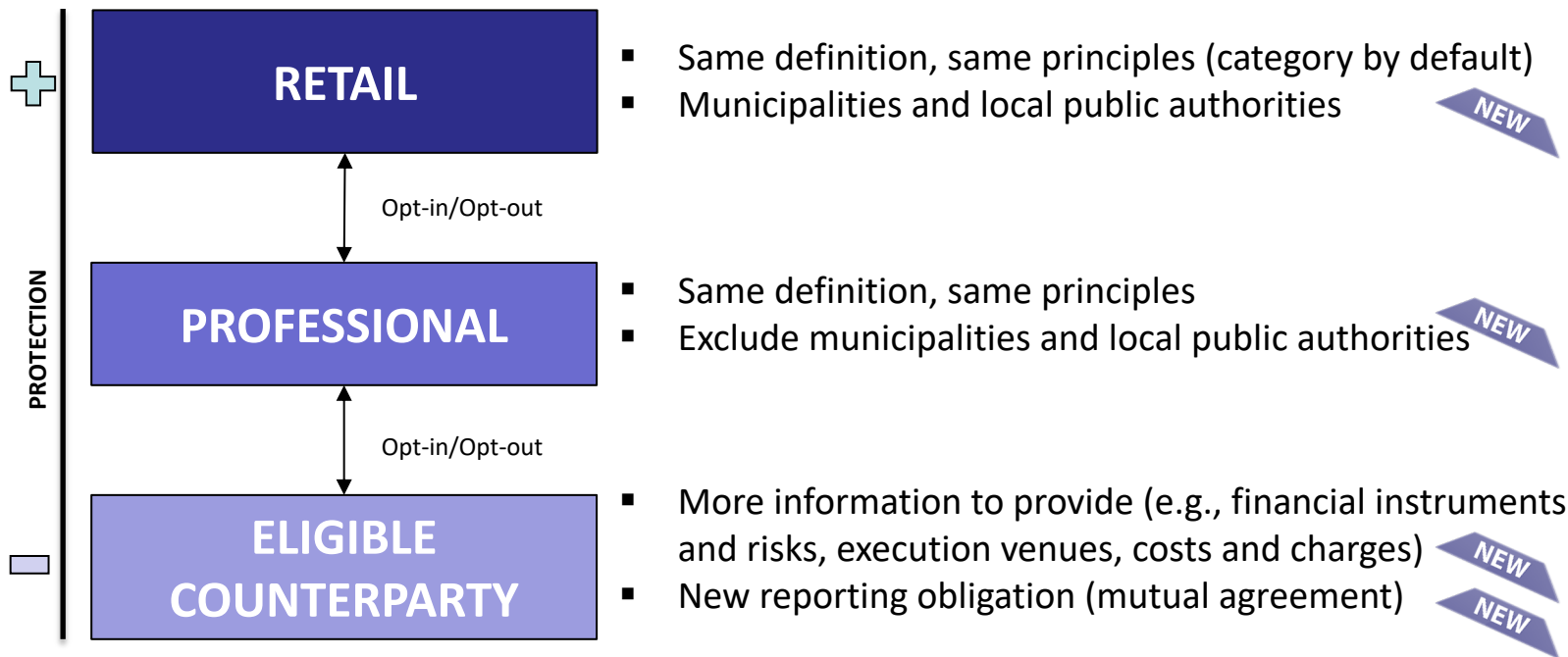
2. MiFID II Key concepts





2.1 Client Classification

- **Basic principle:** MiFID II does not change the categories of clients, nor the various monetary thresholds and experience levels that eligible counterparties and professional clients are required to meet
- Bespoke changes are made for municipalities and local public authorities as well as for eligible counterparties (in regard of elective eligible counterparties, disclosures and reclassification)





2.1 Client Classification Approach

Professional : “ Client who possesses the Experience, Knowledge and expertise to make his own investment decision and properly assess the risks that it incurs.

Financial Professional Assumptions
(individual basis)

MIFID I

- Balance sheet total: € 20.000.000
- Total Net Turnover: €40.000.000
- Own Funds: €2.000.000



MIFID II


- SMEs ?
- Municipalities vs Regional government
- ECP : general duty of loyalty
- Opt-UP/Down rules : Pro (~~K&E~~) → Retail
- Small pension funds

Retail : *Not professional*

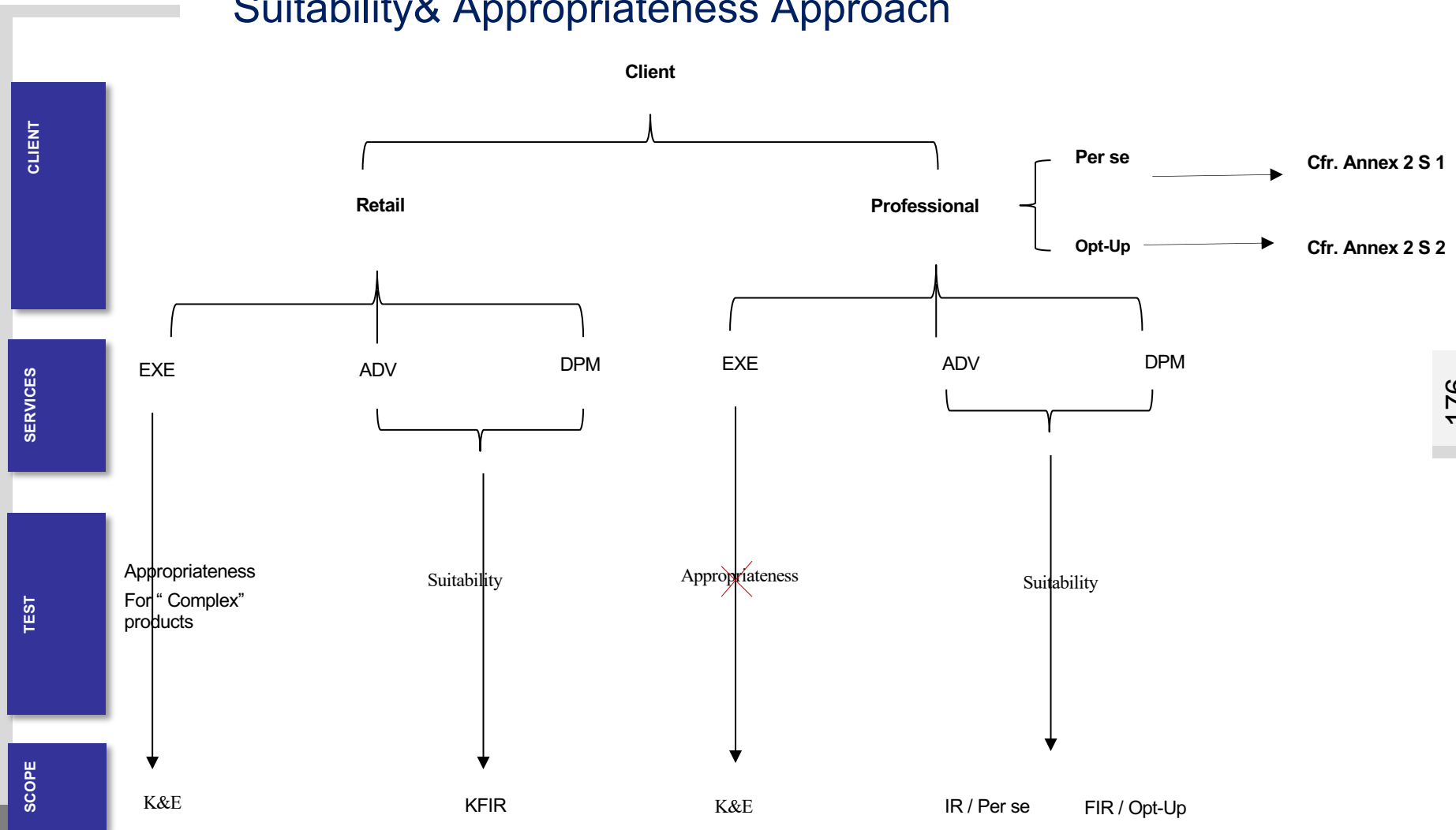
ECP: *Market players with sophistication similar to financial intermediaries*



2.2 Client Profiling

- Client profiling is based on the following criteria:
 - **K**nowledge and experience
 - **F**inancial situation
 - **I**nterest objectives
 - **R**isk tolerance
-  Responsibility of financial institutions only
- Signature of the Client is required

Suitability & Appropriateness Approach



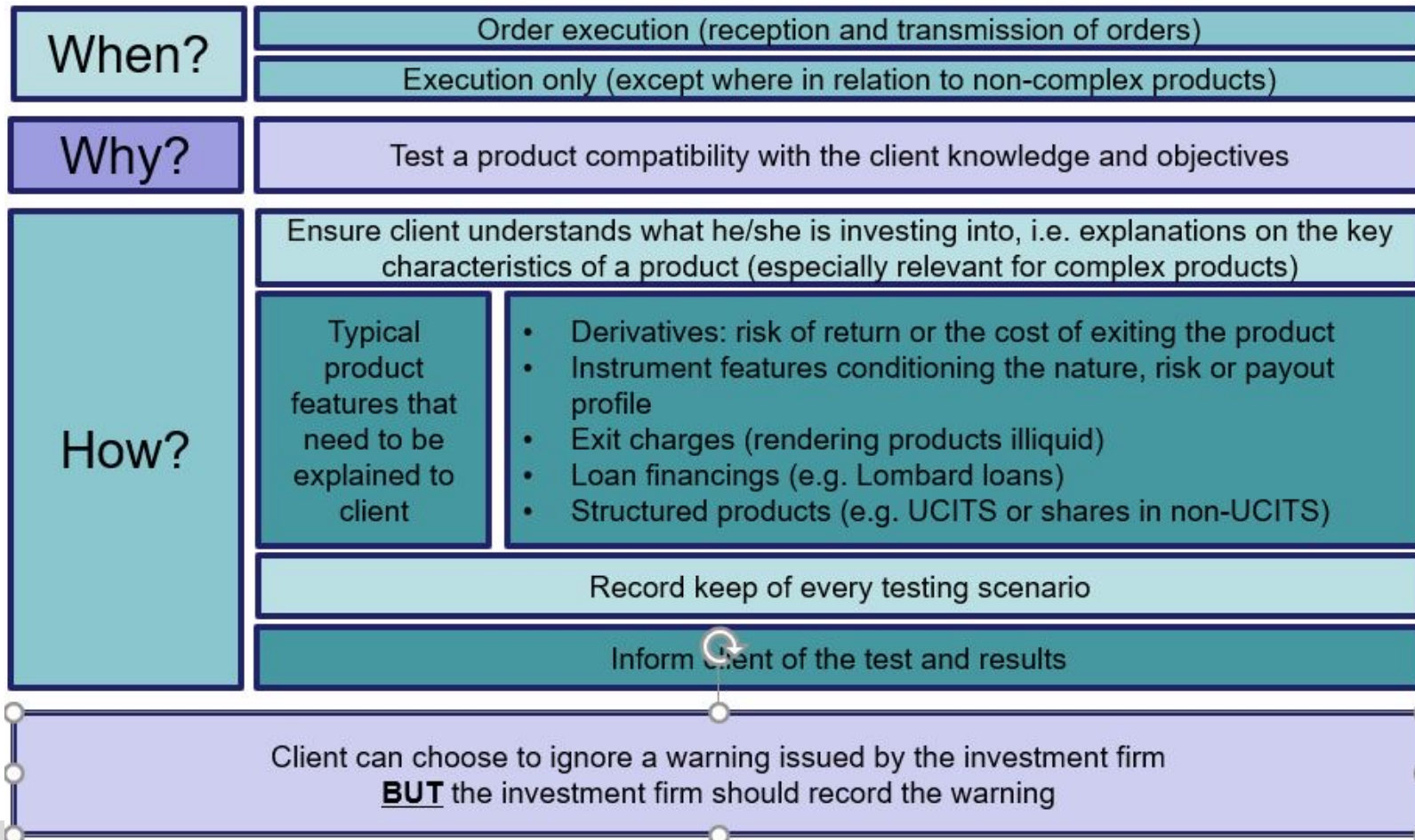


2.3 Client Tests: Suitability

When?	Investment advisory services (independent or not)				
	Portfolio management relations				
Why?	Understand client objectives and goals				
	Align service provision with client objectives and goals				
How?	Test client goals and objectives against the proposed investment service and/or financial instrument				
	Test all client interactions (buying, selling and holding) based on 4 criteria:	<ul style="list-style-type: none"> • Knowledge and experience • Financial situation (including ability to bear losses) • Investment objectives • Risk tolerance 			
	Record-keep every testing scenario				
	Inform the client about the test and the results				
	The investment firm can never ignore a negative suitability test and proceed (blocking suitability), even at the client's insistence with a transaction or service that is not suitable				
<table border="1"> <tr> <td>In practice: Deep analysis on first contact, then updates</td> <td>Firms to provide client with ex-ante suitability report specifying the advice given and how it meets the preferences, objectives and other client characteristics (similar to German <i>Beratungsprotokoll</i>)</td> <td>For Discretionary Portfolio Management: suitability report can be part of the portfolio management report</td> </tr> </table>			In practice: Deep analysis on first contact, then updates	Firms to provide client with ex-ante suitability report specifying the advice given and how it meets the preferences, objectives and other client characteristics (similar to German <i>Beratungsprotokoll</i>)	For Discretionary Portfolio Management: suitability report can be part of the portfolio management report
In practice: Deep analysis on first contact, then updates	Firms to provide client with ex-ante suitability report specifying the advice given and how it meets the preferences, objectives and other client characteristics (similar to German <i>Beratungsprotokoll</i>)	For Discretionary Portfolio Management: suitability report can be part of the portfolio management report			

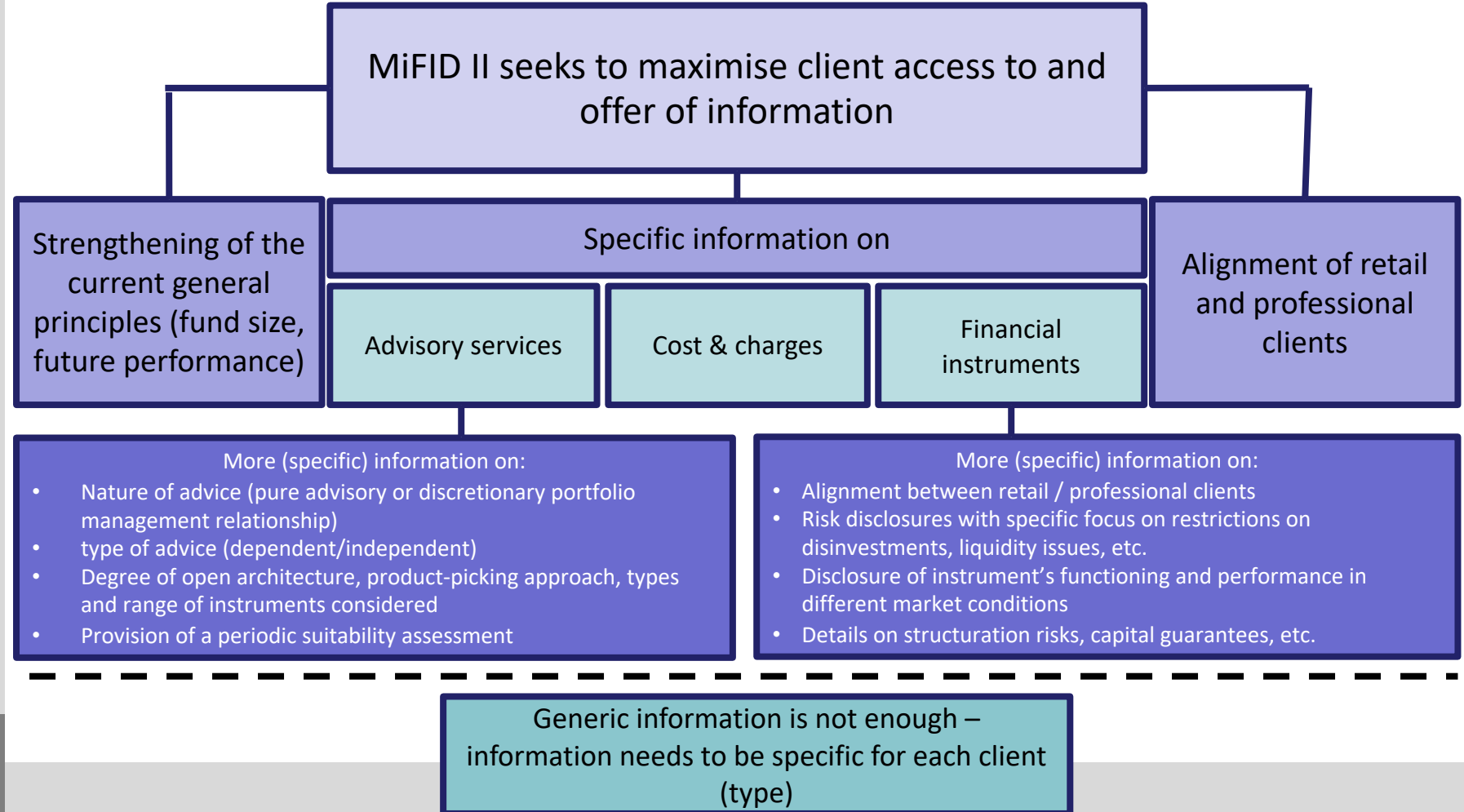


2.4 Appropriateness





2.5 Information to Clients (1/2)





2.6 Information to Clients (2/2) – Cost and charges

Principle:

Cost and charges information must be provided to all clients (with minor exceptions)

Ex-ante and ex-post information on:

- Costs of the firm and costs of relevant instrument (i.e. what does it cost to invest in a certain product with a certain firm)
- Retrocessions and inducements (considered as a cost for an investment service)

Presentation of this information

- Aggregated as initial/on-going/exit costs
- In EUR and in percentages against the investment

Specificities of ex-ante information:

- Simulated figures or
- Proxy for likely figures
- Generic figures (if representative)
- Including illustrations of costs on return

Specificities of ex-post information:

- Actual costs incurred
- At least annually
- Match the ex-ante figures communicated to client



- Mark-ups in FX or FI trading
- Instruments costs include firm management fee, fund management fee of the fund, as well as brokerage



2.7 Commissions (Retrocessions) and Inducements


**NO
INDUCEMENT**

Independent advice

Portfolio Management

Also applicable to:

- Brokerage fees (whether received or paid)
- "Free" research (needs to be paid by firm or client)

If received: return immediately to clients in full (based on policy)

Also applicable for non-monetary benefits (when non-minor*)

* Minor non-monetary benefits are tolerated, with ex-ante disclosures: to be clearly disclosed before providing services to clients

Inducements permitted

Reception and transmission of orders

Execution only

Non-independent advice

Business introduction

External asset managers

if

Full transparency (ex-ante and ex-post) via reporting (not only disclosure)

+

No conflicts with client interests

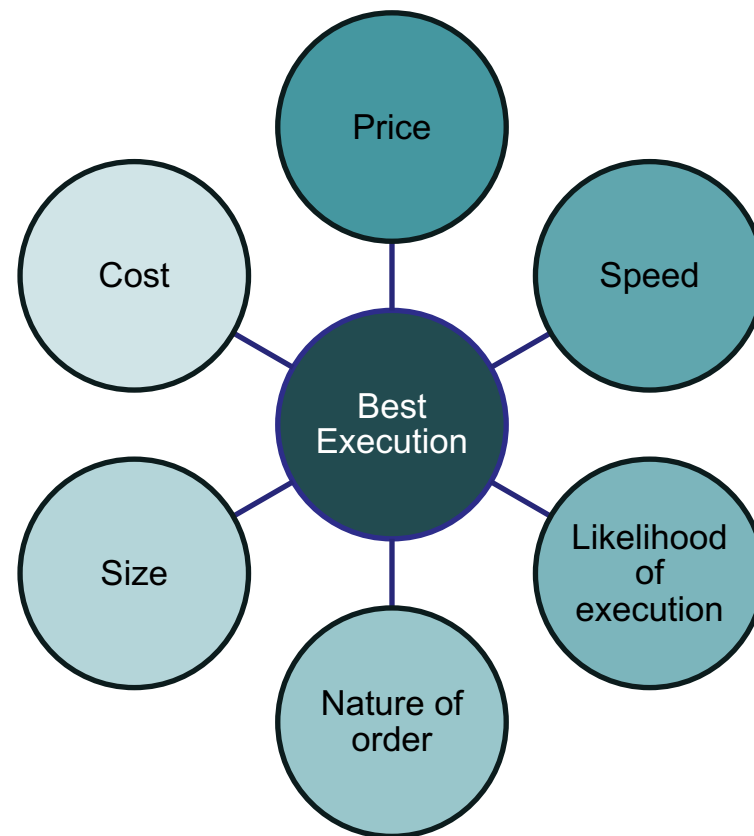
+

Justification: enhancement test and inventory (specific)



2.8 Best Execution

- Unchanged in its principle: “total consideration”, “best possible results”, execution versus RTO/selection policies.
- Strengthen principles
 - More detailed and more practical execution policy to clients, explaining clearly how orders will be executed by the firm (factors, venues / entities used) per instrument type
 - Link to most recent execution quality data
 - Use of a single venue: challenged, need to demonstrate, with figures
 - Details on situations out of RM/MTF/OTF
- Effective monitoring
 - Must become a reality: monitor effectiveness, assess on a regular basis, inform existing clients of material changes
 - Review the policy at least annually
 - Get data





3. Governance & Supervision





3.1 MiFID II Governance

MiFID II imposes a set of rules and obligations relating to the internal setup, organisation and governance of investment firms when providing investment services

Aim

- Assimilate (to the extent necessary), investment firms to other type of firms active in the financial markets, namely credit institutions
- Enhance investor protection and transparency by requiring investment firms to proceed in information exchanges with other market participants with whom they transact or use of products along with clients

Main areas of concern

- Product governance (information exchange between product manufacturers and distributors)
- Best execution (client information), clients' complaints (procedural set-up)
- Internal organisation and governance (staff training and governance set-up) and conflict of interests management
- Organising client relationship from a governance perspective (client contact and signature)



3.2 Supervision & Sanction Regime

SUPERVISION

- Additional power to NCA, e.g., require information about size and purpose of a position or an exposure entered into via a derivative and any assets or liabilities in the underlying market
- Clearly provides minimum set of remedies in case of issues, e.g. requirement of cessation of any practice, freezing or sequestration of assets, suspension or removal of/from trading.
- Power to ESMA or NCA or EBA to temporarily prohibit or restrict (including on precautionary basis):
 - Marketing, distribution or sales of particular financial instruments or types of instruments
 - A type of financial activity or practice

SANCTIONS

- Member States to decide on sanctions**, following EU guiding principles:
- Public statement, indicating the person/entity and nature of breach
 - Order to cease the conduct
 - Withdrawal or suspension of the authorization (incl. for Reporting entities)
 - Temporary or permanent ban against persons in management body
 - Temporary ban of an IF as member of a market venue
 - Legal person: pecuniary sanctions of up to 10% of annual turnover for legal persons

Physical person: up to 5 million EUR or up to twice the amount of the benefit derived from the breach

Sanctions and measures applied should be published (with related details, e.g. type, persons)

Appropriate mechanisms to encourage reporting of breaches within investment firms



Case Studies



Case Study 1

- A grandmother (80 years old) and her grandson (25 years old) come to the bank to open an account together. When establishing their risk profile, the outcome for the grandmother is “conservative” and the outcome for the grandson, “aggressive”.
 - They want to have an advisory service for which they both can make investment decisions based on your advice. The grandmother thus wants to help her grandson with his “financial education”.
 - The grandson wants to be very active and therefore proposes to opt for an aggressive strategy.
- ***How do you approach this situation?***



Case Study 2

- An existing client of your bank, a very busy real estate developer, has an account for which he normally receives advice. He has a “medium” strategy and has always had a “buy and hold” approach.
 - Recently he added his sister as a proxy on the account.
 - She has a degree in economics and works for an insurance company. She wants to be more active with the account and starts entering at least 2 orders each week.
 - Furthermore, she has plans to invest part of the portfolio in options and commodity futures in order to improve the portfolio's performance.

- ***How do you approach this situation?***



Case Study 3

- You work for bank Green Frog, a subsidiary of the Green Frog Group, listed on Euronext.
 - Your client is interested in reinvesting the dividends that were recently paid to his account.
 - There is a market consensus between analysts that Green Frog has interesting perspectives and will probably have a dividend yield well above market average.
- ***Would you advise your client to purchase Green Frog shares?***



Case Study 4

- Your client has a moderate risk profile and is holding about 5% of his portfolio in cash.
 - When preparing for your next meeting with the client, you notice that based on his current asset allocation the client could invest this cash in shares.
 - Based on the research of your bank, you recommend the client to invest in a new European telecommunication company, which has very strong potential.
 - The client is very enthusiastic and wants to sell his money market funds, which represent 20% of his portfolio, in order to invest a total of 25% of his portfolio in the telecommunication shares.
- ***How do you approach this situation?***



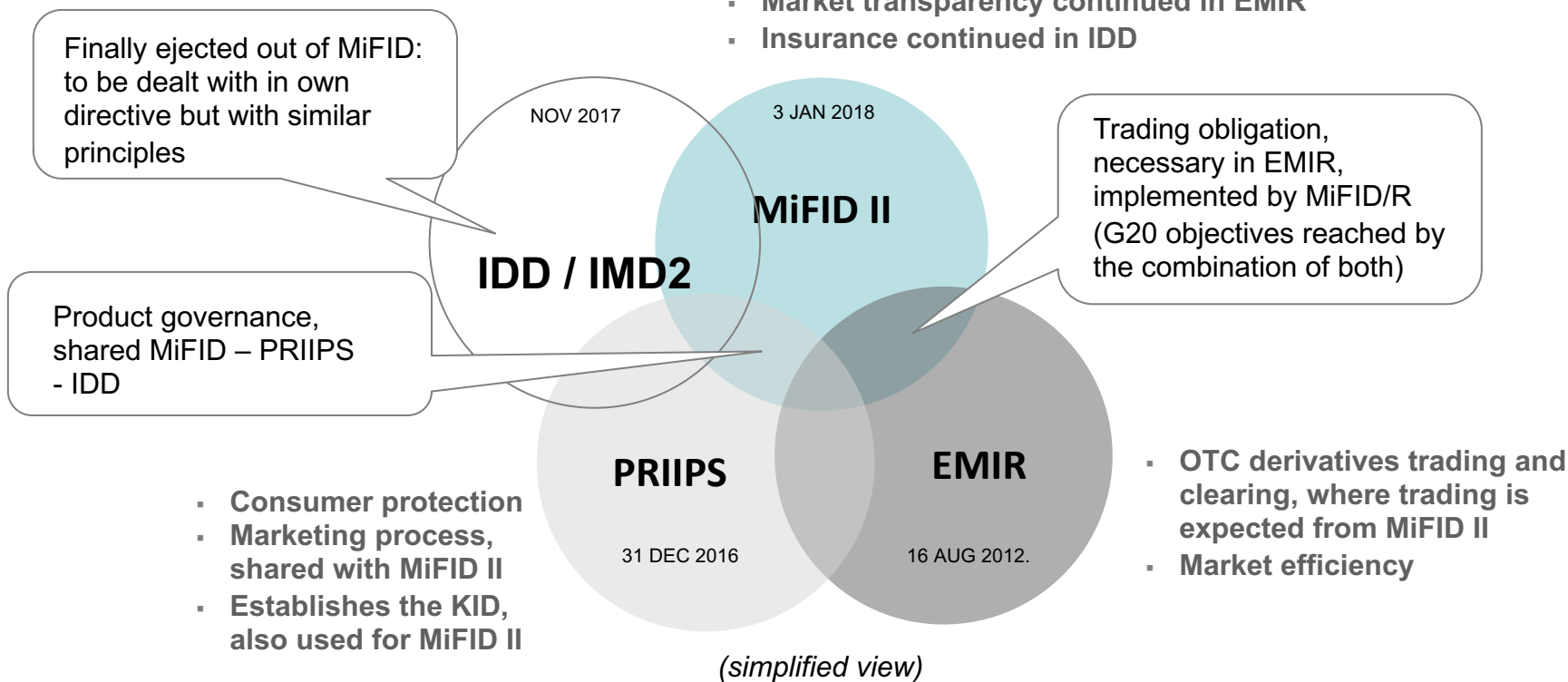
Case Study 5

- Your client has given you an order to sell his position in shares 123.
- Immediately after you introduce the order in the system, your dealing room calls you to warn you that the order represents 60% of the average daily volume.
- ***How do you approach this situation?***

Towards the same objectives

Consumer protection + Market Transparency

- Evolution of MiFID, with a strong emphasis on markets
- Conduct of business
- Market organization
- Customer protection continued in PRIIPS
- Market transparency continued in EMIR
- Insurance continued in IDD



And other links with UCITS IV, MAD2, CRD, etc.



Complex vs. Non-Complex Instruments

- The basic approach in MiFID II is that complex financial instruments should only be sold to qualified investors, while retail investors should only invest in non-complex instruments
- The main differences between non-complex funds and complex funds can be summarised as follows:
 - UCITS funds are non-complex and thus suitable for all types of investors
 - Alternative funds (i.e., non-UCITS funds) are complex instruments



Best Execution

(MiFID II – L1D 27-28, rec.97 / L2DR 64-66)

- ❑ Expect a **more detailed and more practically focused execution policy summary to clients**, explaining clearly how orders will be executed by the firm and how the selection is made:
 - List the factors used to select a venue for execution and the entity used for transmission or placing orders and their relative importance (and consistency with monitoring approach)
 - How venue selection occurs, specific execution strategies used, the process used to analyze the execution quality, how the firm monitors the achievement of the best possible result
 - List the venues/entities used for execution/transmission/placing clients orders in the policy, specifying which venues/entities are used for each class of financial instrument
 - Clear, meaningful, to effectively understand how and where orders are executed
 - Distinguish between types of clients, instruments, orders
 - Explaining special situations (e.g., use of internal matching systems, a single venue, execution outside RM/MTF/OTF)



Best Execution

(MiFID II – L1D 27-28, rec.97 / L2DR 64-66)

- ❑ Expect a **more detailed and more practically focused execution policy summary to clients**, explaining clearly how orders will be executed by the firm and how the selection is made (continued):
 - Retail clients:
 - Provide link to the most recent execution quality data published
 - Summary of the policy focused on the total costs client will face
 - Any specifics on the fees charged (e.g., fees charged by the investment firm to all counterparties involved in the transaction and the situation where the fees applied vary with the execution venue or entity, the policy must indicate the maximum fees or range of fees that may be payable)
 - Information about any payment or benefits received from any party in the chain with no breach of the inducement rule



Best Execution

(MiFID II – L1D 27-28, rec.97 / L2DR 64-66)

Executed off-market

Dealing in OTC product

- Check the fairness of the price proposed to clients by gathering market data used for the price estimate and by comparing them to similar products where possible

Orders executed outside a RM/MTF or OTF

- If executing party: need express consent (no change, like in MiFID I) before proceeding and in the form of general agreement or in respect of individual transaction.
- If RTO: need to explain in the policy the main execution principles used by the other entities and to provide appropriate information about those entities upon client request
- Clearly stated in the policy with additional information on the risks of this way of execution and the counterparty risk (seen as “new” since bilateral). On request, more consequence in terms of counterparty risk.



Best Execution

(MiFID II – L1D 27-28, rec.97 / L2DR 64-66)

❑ Client order handling rules

- No change: principle designed in MiFID I is confirmed by MiFID II L1 and L2
- More details required in the Best Execution (BEX) policy reflecting Client Order Handling arrangements, e.g., handling of limit orders (standard, large size, which venue, what if, etc.)

❑ Single execution venue / entity

- Use of a single execution venue: Must show how it satisfies the BEX requirements and the results must be at least as good as with other entities
-> must be grounded on data and internal analysis



Best Execution

(MiFID II – L1D 27-28, rec.97 / L2DR 64-70)

☐ Monitoring

- To monitor the effectiveness of the execution arrangements
- To assess on a regular basis whether the execution venues still qualify to provide the best possible results
- To inform the existing clients of material changes
- On client request, to be able to demonstrate compliance with the execution policy
- BEX policy to be reviewed at least annually and in case of material change
- To organise the review on the same aspects as laid out in the policy

☐ Additional disclosures

- Make public on an annual basis for each class of instrument:
 - The top 5 venues in terms of trading volumes where they executed client orders in the preceding year
 - With Information on the execution quality obtained for each one



Transaction Reporting

(MiFIR – L1R 26, RTS22)

- ❑ For **all trading venues** (RM, MTF,OTF) and not only instruments that can be traded on a RM
- ❑ For **all instruments somehow related to a trading venue**:
 - Instruments admitted to trading or traded on a trading venue or for which a request for admission has been made
 - Instruments for which the underlying financial instrument is traded on a trading venue
 - Instruments for which the underlying is an index or basket composed of instruments traded on a trading venue
- ❑ For **acquisition or disposal of above-mentioned financial instruments**:
 - Purchase or sale of a financial instrument
 - Enter into or close out a derivative contract in a financial instrument
 - Increase or decrease in the notional amount for a derivative contract that is a financial instrument
 - Detailed list of activities which do not constitute a transaction under the meaning of Art 26 of MiFIR and Del. Reg. 2017/590 – Art 2(5) – RTS 22
 - Regardless of whether or not the transaction was made on a trading venue



Transaction Reporting

(MiFIR – L1R 26, RTS22)

- ❑ Clear definition of reported transactions and fields (**RTS 22 Annex 1**), with common European standards and format (i.e., XML template in accordance with ISO 20022 methodology)
- ❑ Information going further than just trade related, including (among others): the identification of any applicable waiver, short sale, risk effect for commodity derivatives, identification of clients and the trader / the person responsible for the execution of the client order, the computer algorithm responsible for the decision, etc.
- ❑ Obligation for RTO (all entities in the chain) to pass on the complete information when sending an order to another firm OR to report themselves after execution (issue: client confidentiality)



Reporting to Clients

(MiFID II – L1D Rec 104, Art 25.6, 30-1 / L2 DR 59-63)

Extended to all clients

Portfolio management reports

- Activities undertaken and performance over the period
- Frequency : from 6 months to quarterly (or access to the online system)
- Loss : where the NAV depreciates by 10% or more and at multiples of 10% within 24 hours and immediately for derivatives

NEW

Periodic statements

- Frequency : from 6 months to quarterly (more frequent on request)
- Identification of assets subject to MiFID protections
- Market or estimated value of the instruments

Leveraged financial instruments

- Loss : where the value of a position depreciates by 10% or more and at multiples of 10%

NEW



Conflicts of Interest (Col)

(MiFID II – L1D 16.3, 23/ L2DR 33-43)

- ❑ **Specific situations to be specifically addressed in the Col Policy:**
 - Impact of receipt of inducements
 - Col caused by remuneration or other incentive structure
 - Col caused by the way the performance of the staff is assessed • Sales commissioning
- ❑ **Other details about disclosure of potential Col to clients (also to non-retail clients)**
 - In a durable medium
 - Before the provision of service
 - With a specific description of the Col, including enough detail for the client to make an informed decision (nature, source of conflict, risks, mitigation measures)
 - Clearly stating that the current arrangements have not been sufficient to prevent the risk



Conflicts of Interest

(MiFID II – L1D 16.3, 23/ L2DR 33-38-43)

❑ Periodical review, at least annual review

❑ New requirements for investment research

NEW

- Physical separation between financial analysts involved in the production of investment research and other relevant persons whose responsibilities or commercial interests may conflict with the interests of clients or third parties
- If the requirement is not appropriate to the firm (size/nature/scale and complexity of business), alternative information barriers shall be put in place

❑ Specific requirements under L2 for the underwriting and placing activities

NEW

- Specific information to provide when advising corporate finance strategy
- Impacts on underwriting and placing (including pricing)



Inducement

(MiFID II – L1D 24.4, 24.7-9, Rec 73-76 / L2 DD 11-13)

❑ Definition

- Commissions or non-monetary benefits paid or received/given from/to third parties in relation to an investment service to a client and which are not seen as « proper » or « standard » fees (i.e., necessary to the delivery of the service)

❑ Minor non-monetary benefits

- No list defined by EU yet
- Information or documentation relating to a financial instrument or an investment service (generic in nature or personalised to reflect the circumstances of an individual client)
- Material written by a third party sponsored and paid for by a corporate issuer or a potential issuer to promote a new issue of the company
- Participation in conferences, seminars and other training events on the benefits and features of a specific financial instrument or an investment service
- Hospitality of a reasonable *de minimis* value (e.g., food and drink during a business meeting or a conference, seminar or other events)

=> ***to be clearly disclosed before providing services to clients***



❑ Recording client conversations

MiFID II – L1D 16.7 + Rec 57 / L2DR 76

- Recording phone and electronic communications when
 - Transactions concluded when dealing on own account
 - Clients orders, in RTO or in execution services
 - From reception of order to conclusion of the transaction, including cancellations or modifications -> ability to trace back the entire flow of communications
 - Any conversations or communications intended to result in such transactions, even if they did not result in such transaction
- Not applicable to private device
- If face-to-face: written minutes



☐ Employees knowledge and competences

MiFID II – L1D 23(1), 24(10), 9(3), 29, 73, Rec.53 / L2DR 27

- Trained & Competent & Independent
 - **Circular CSSF 17/665**
 - Appropriate level of knowledge and competence in relation with the products (when advising or selling to retail clients)
 - Annual review of staff assessment
 - Review of the remuneration policy
- Distinction between staff providing **information** and staff providing **advice**

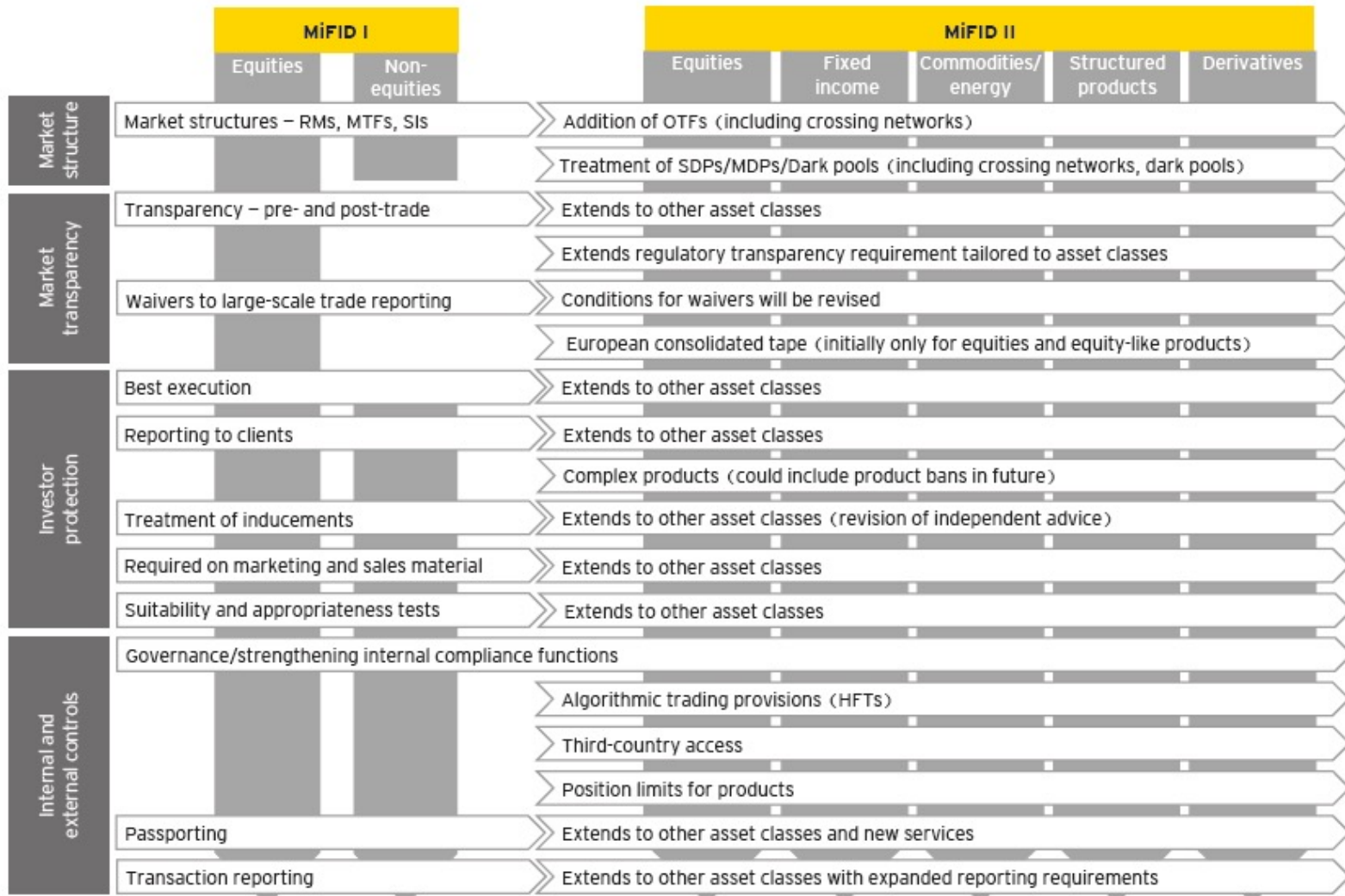


Product life-cycle - requirements





MiFID I, II and Instrument Types*



*Ernst & Young, *The World of Financial Instruments is More Complex* (2015)



4. Conclusion





- MiFID I set the framework, MiFID II expands the framework
- MiFID II is a commercial challenge and an opportunity
- MiFID II is definitely an organisational challenge
 - Ability to assess on a continuous basis the client and inform the client about new products or about its portfolio (which could be arranged contractually)
- MiFID II requires revisiting the entirety of the operating model



Document everything!

Proper record-keeping will be your (only) protection



Do not consider it as a pure compliance exercise;
there are commercial and business opportunities



- COMPLIANCE, GENESIS & KEY PRINCIPLES
- COMPLIANCE FUNCTION FUNDAMENTALS
- FINANCIAL CRIME FRAMEWORK
- INVESTOR PROTECTION : MIFID OVERVIEW
- DATA PROTECTION**

Data Protection



Data Protection

Agenda

1. Definitions
2. Main principles
3. Supervision by the Data Protection Authority (DPA)
4. GDPR & Directive
5. Data Controller & Data Processor
6. Data governance key stakeholders
7. Data subject rights
8. International personal data transfers
9. Outsourcing in the financial sector
10. Data breach management
11. Sanctions
12. Enforcement actions
13. Practical cases



1. Définitions (1/5)



Personal data : Any information relating to a natural person who is or can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to him/her.

Name	Photography	E-mail address
Tax Identification Number	IP address	Phone number

The data collected must be proportional to the purposes of the data processing. Special categories of personal data (ex “sensitive data”) processing is strictly regulated.

Biometric data	Racial or ethnic origin	Identification data
Sexual Orientation	Medical data	Criminal Offense



1. Definitions (2/5)

To what special categories does personal data belong?

- Examples (not exhaustive):
 - Racial or ethnic origin, political opinions, religious or philosophical beliefs
 - Membership of a trade union
 - Physical or mental health, sexual life
 - Data submitted to specific regulations (financial data, medical data, ...)
 - Social security number/national identification number
 - Judicial data, criminal offences
 - Time series, log-data, tracking-data, data representing interactions or activities and data representing a behaviour might also be sensitive
- Handling of ‘special categories of personal data’ is strictly regulated /limited (processing Art. 9 - GDPR)



1. Definitions (3/5)



- **Data Subject** : Any individual about whom personal data is processed

Natural person

Personal data

Resident or
Citizen

Activities of
processing

The extraterritorial clause means that the GDPR applies to Citizens (regardless of their location), residents (while residing), when the controller/processor is established in the EU, when personal data refers to goods of services or monitoring behaviour of EU Data Subjects, or Controller is not established in the EU, but given its nature EU Law applies (e.g. Embassy)



- **Processing** : Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.



1. Definitions (4/5)



- **Personal data processing** : Processing personal data means any action taken in conjunction with personal data (regardless of the level of automatisation):



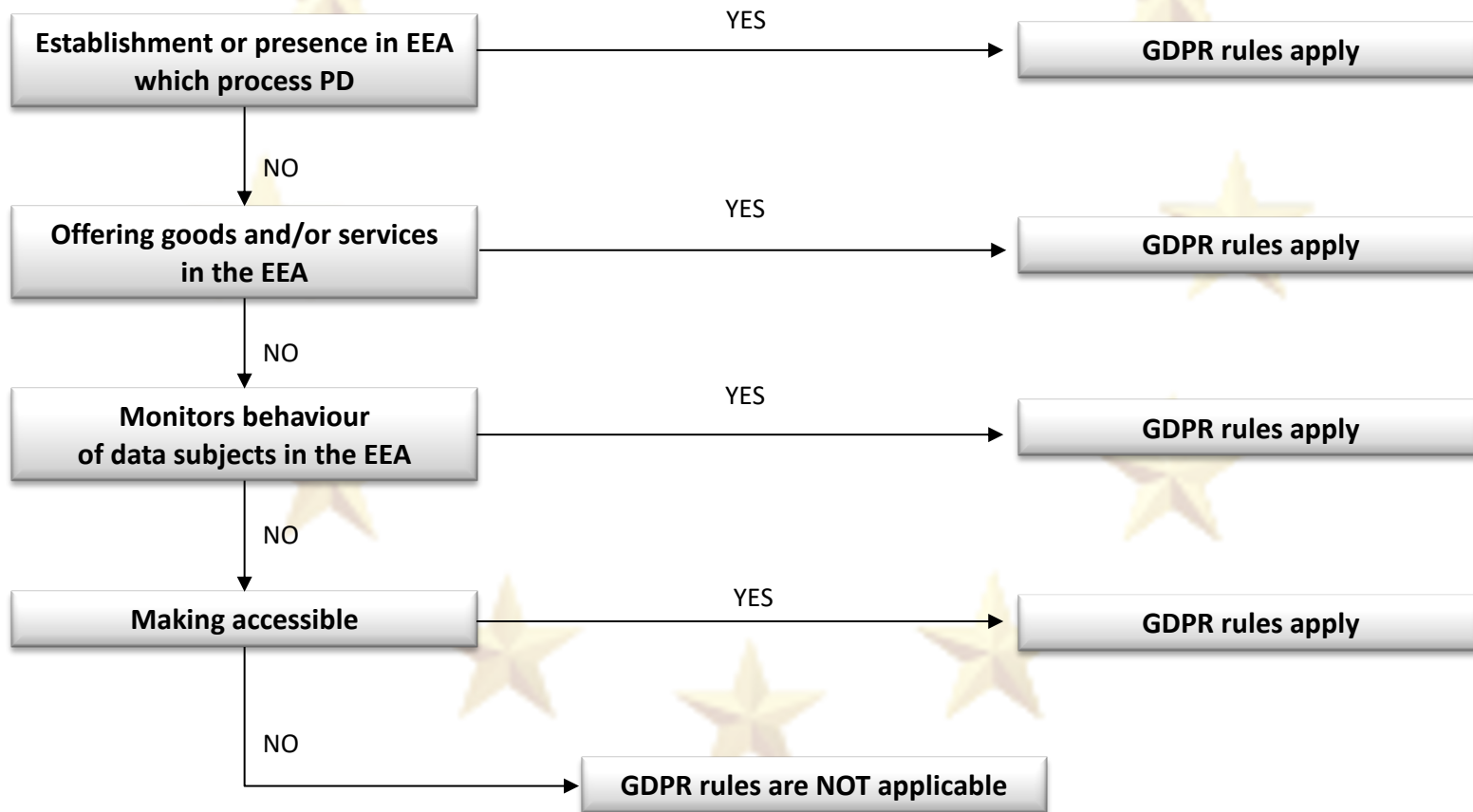
- **Roles** : natural or legal person, public authority, agency or any other body ...
- **Controller** : Determining the purposes and means of the processing of personal data. If more than one person is to be held as named controller, they will be defined as *joint controllers*.
- **Processor** : Processing personal data on behalf of the controller (instructions)



1. Definitions (5/5)



Data Protection rules applicability test:





2. Main Principles (1/3)

- 1 Transparency: Data should be processed fairly and lawfully
- 2 Purpose and lawfulness: Data should be obtained only for one or more specified and lawful purposes and the processing must have a legal ground (out of the 6 listed by Art. 6 GDPR)
- 3 Relevancy: Data should be adequate, relevant and limited to the purpose for which it is of processing
- 4 Accuracy: Data should be accurate and up to date
- 5 Data retention: Data should be kept for only as long as necessary/lawful (register of data)
- 6 Rights: Data should be processed in accordance with the rights of data subject (as applicable)
- 7 Information security: Adequacy of means: Data should be kept secure (physical and technically)



2. Main Principles – Lawfulness Art 6 (2/3)

- (a) the data, the subject has given consent to the processing of his or her personal data for one or more specific purposes;
- (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
- (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.



2. Main Principles – Lawfulness Art 6 (3/3)

Article 4 Nr. 11 – Definitions

- **‘Consent’** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
- **Legitimate interest** (of the controller or third party)
 - Is not defined as is the most flexible lawfulness available.
 - It requires understanding of why the party should process and how his interest has higher relevance than the data subject right (balance of interest test)
- **Elements to proceed :**
 - identify a legitimate interest
 - show that the processing is necessary to achieve it
 - balance it against the individual’s interests, rights and freedoms
 - conclude its applicability



3. Supervision by the Data Protection Authority (DPA)

DPA powers / obligation

- Power of investigation
 - The DPA is allowed to access data being processed. It has direct access to the premises, unless they are residential premises, where the data is processed and to the data being processed, and carries out necessary checks
- Power of sanction
 - The DPA has the possibility of adopting a number of administrative sanctions, and disciplinary sanctions (alert, admonish controllers, block, delete, destroy data, impose temporary or definitive ban on a processing, order publication of the prohibition decision)
- Obligation of producing guidelines
 - The DPA is tasked with producing guidelines and to cooperate with other DPAs



4. GDPR + Directive (EU) 2016/680 [1/3]

Objective: To give citizens control over their personal data and to simplify the regulatory environment for business

Directive (EU) 2016/680

Member States shall adopt and publish, by 6 May 2018, the laws, regulations and administrative provisions to comply with this Directive

Protection of natural persons with regard to the **processing of personal data by competent authorities** for the purposes of the prevention, **investigation, detection or prosecution of criminal offences or the execution of criminal penalties**, and on the free movement of such data

General Data Protection Regulation (EU) 2016/679

No transposition into national law
Applicable and binding since **25 May 2018**

Harmonisation of rules within the European Union
Enhance cooperation between the national authorities of the 28 Member States
Lawfulness for processing



4. Data Protection – New European Directive (2/3)

Directive: Increased exchange of data between police and judicial authorities

- The Directive applies to the cross-border processing of personal data, as well as to the processing of personal data by police and judicial authorities at strictly national level. Accordingly, police and judicial authorities should no longer apply different rules according to the origin of the personal data
- Transferring personal data from competent authorities to private entities is made possible under specific conditions. This allows police authorities to take swift action in cases of a terrorist attack or other emergencies
- Police authorities are now allowed to limit both the information held in on the data and access to the processed data. The framework allows for police authorities to neither confirm nor deny whether they are in possession of personal data in order to avoid compromising on going investigations.



4. Data Protection – New European Regulation (3/3)

Regulation : Increase protection of natural persons with regard to processing of personal data and on the free movement of such data.

- New data subject rights : (i) data portability (ii) right to be forgotten (iii) right to object (iv) right to object to automated decisions and profiling
- New data controller obligations : (i) data repository/register creation, (ii) data impact assessment implementation
- Obligation to appoint a Data Protection Officer : Under certain conditions
- Further responsibilities of Data Processors e.g. assistance, reporting to controller, submission to instructions
- Large increase in financial administrative sanctions e.g. Suspending or interrupting processing



5. Data Controller (DC) & Data Processor (DP)

- **Data Controller**: A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed.
 - Legitimacy and lawfulness of processing personal data
 - The controller must have legitimate reasons for carrying out the planned processing
 - Purpose has to be determined **before** the processing begins, has to be **specified** and **explicit** and **legitimate**
 - Data retention: only for the period of time necessary for the purpose of the processing. Once fulfilled, the data should be removed (except if data is “anonymous” as it is not personal data anymore)
 - Respect of the data subjects' rights (information about processing, having access on request, ability to object)
 - Data security and confidentiality measures (processing, sub-contractor, protection of data by appropriate technical and organizational measures)
- **Data Processor**: Any person (other than an employee of the data controller) who processes the data on behalf of the data controller. Execution of instructions (responsibility for executions and assistance).



6. Data Governance Key Stakeholders

Chief Data Officer

- **Highly recommended**
- where the core activities involve regular and systematic **monitoring of data subjects** on a **large scale**
- processing of **special categories of data** at large scale.
- CDO shall directly report to the highest level of management
- CDO shall support the DPO in the execution of his/her tasks.

Data Protection Officer

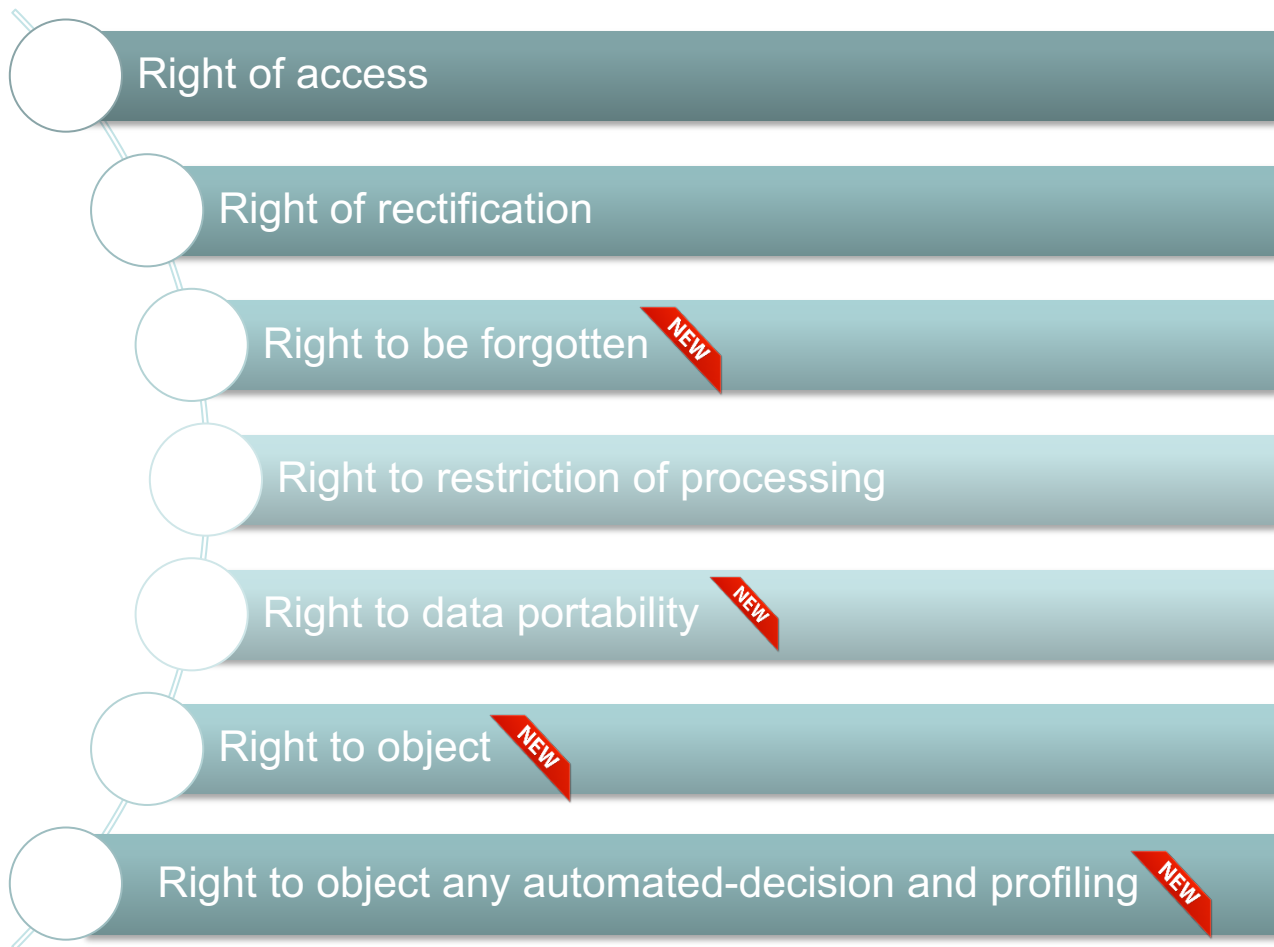
- **Required by GDPR where:**
- processing is performed by a **public authority**
- where the core activities involve regular and systematic **monitoring of data subjects** on a **large scale**
- processing of **special categories of data** at large scale.
- DPO shall directly report to the highest level of management
- Controller/processor shall support the DPO in the execution of his/her tasks
- role of coordination

Chief Information Security Officer

- Senior-level executive responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected
- Respond to incidents, establish appropriate standards and controls, manage security technologies, and direct the establishment and implementation of policies and procedures



7. Data subjects rights (1/9)





7. Data subjects rights (2/9)

7.1. Right of access

Obtain from the controller confirmation as to whether or not personal data concerning a data subject is being processed, and, where that is the case, access to the personal data and the following information:

- the purposes of the processing
- the categories of personal data concerned
- the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that data retention period (document retention has as impact data retention)
- the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing (limited right)
- the right to lodge a complaint with a supervisory authority
- where the personal data are not collected from the data subject, any available information as to the data source
- when applicable, the existence of automated decision-making, including profiling

The right of access may be limited by other regulations (e.g. Suspicious activity/transaction report)



7. Data subjects rights (3/9)

7.2. Right of Rectification

- Obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her.
- Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.
- The right of rectification should be read in coordination with the principles of:
 - accuracy of data
 - relevance (completeness) and
 - obligation of keeping data up to date



7. Data subjects rights (4/9)

7.3. Right to be Forgotten

Obtain from the controller the erasure of personal data concerning the data subject without undue delay where one of the following grounds applies:

- the personal data is no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- the data subject withdraws consent on which the processing is based, and where there is no other legal ground for the processing;
- the data subject objects to the processing and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing;
- the personal data has been unlawfully processed;
- the personal data has to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
- the personal data has been collected in relation to the offer of information society services.



RETENTION PERIOD



2014 Google vs Spain case

- In March 2010, Spanish national Costeja González brought a complaint before the country's Data Protection Agency against *La Vanguardia* newspaper, Google Spain, and Google Inc.
- Claim: remove or alter the record of his 1998 attachment and garnishment proceedings so that the information would no longer be available through Internet search engines.
- Google Inc./Spain, to remove or conceal the data.
- Proceedings had been fully resolved for several years and therefore they should no longer appear online.
- The Agency dismissed the complaint against the newspaper on the ground that the publication was legally justified pursuant to a government order.
- Upheld the complaint against Google, finding that Internet search engines are also subject to data protection laws and must take necessary steps to protect personal information
- CJCE established that users can ask search engines to hide certain URLs from search results when a search is conducted using their name and the content on the page the URL points to includes information that is “inadequate, irrelevant or no longer relevant, or excessive.”



- The right to be forgotten gives individuals the ability to exercise control over their personal data by deciding what information about them should be accessible to the public through search engines. It does not, however, give users the power to demand that the personal data be deleted from a site
- Google is regarded as a “**controller**” with respect to “processing” of personal data through its act of locating, indexing, storing, and disseminating such information
- To guarantee the rights of privacy and the protection of personal data, operators of search engines can be required to remove personal information published by third party websites.
- But the data subject’s right to make that request must be balanced against the interest of the general public to access his or her personal information.

➤ Challenges?



7. Data subjects rights (5/9)

7.4. Right to Restriction of Processing

Obtain from the controller restriction of processing where one of the following applies:

- the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data
- the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead
- the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims
- the data subject has objected to processing pending the verification whether the legitimate grounds of the controller override those of the data subject



7. Data subjects rights (6/9)

7.5. Right to Data Portability

Receive personal data concerning the data subject, which the data subject provided to a controller, in a structured, commonly used and machine-readable format and has the right to transmit the data to another controller without hindrance from the controller to which the personal data had been provided, where:

- processing is based on consent or execution of a contract between the controller and the data subject; and
- processing is carried out by automated means (no paper only data)

This includes: emails sent and received, identification data, transactions on a account, internet browsing history

Portability is not absolute over analysis and other proprietary elements linked to the data (e.g. profiling or risk analysis performed by obliged entities)



7. Data subjects rights (7/9)

7.6. Right to Object

Object, on grounds relating to the data subject's particular situation, at any time to processing of personal data concerning the data subject :

- Whenever such data is eligible to be erased
- Whenever such data has been obtained via a law compatible with such right
- Whenever the data is to be transferred out of the EU

The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims (e.g. statutory retention periods, cooperation with authorities...)



7. Data subjects rights (8/9)

7.7. Object to any automated-decision/profiling (1/2)

Right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects the data subject.

This right shall not apply if the decision:

- is necessary for entering into or performance of a contract between the data subject and a data controller
- is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests;
- is necessary for compliance with regulatory obligations of the controller or processor, or
- is based on the data subject's explicit consent (for the period for which that consent is maintained)

... / ...



7. Data subjects rights (9/9)

7.7. Object to any automated-decision/profiling (2/2)

- The controller shall:
 - control the identity of persons concerned
 - in case of doubt, the data controller may request identification documentation
- Information shall be provided in writing, or by other means, including, where appropriate, by electronic means (when requested by the data subject, the information may be provided orally, contingent upon the identity of the data subject being proven by other means)
- The controller shall facilitate the exercise of data subject rights
- The controller shall provide information on action taken on a request to the data subject without undue delay and in any event within one month of receipt of the request (that period may be extended by two further months where necessary, taking into account the complexity and number of the requests)



8. International Personal Data Transfers (1/2)

- Clear distinction between countries which are equivalent or not with regard to data protection (EU Data Adequacy decision)
- Forbidden to non equivalent countries except if the following measures are in place:
 - Appropriate security measures



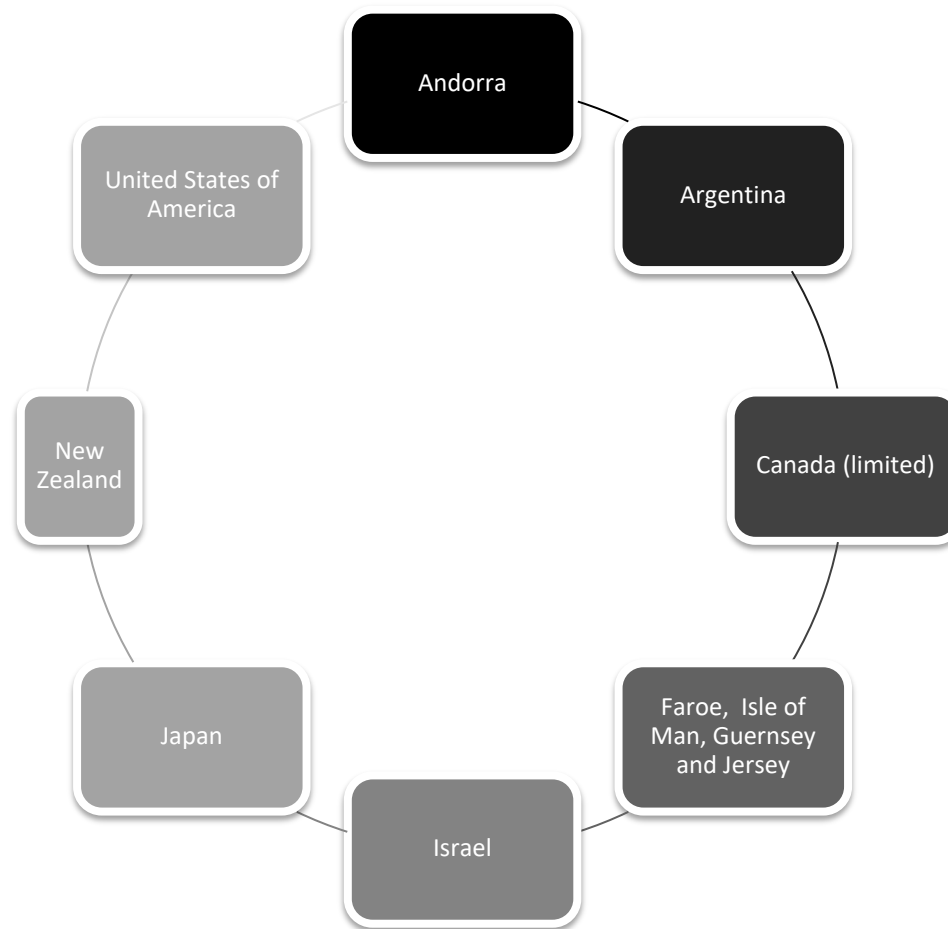
- DPA authorisation
- Prior client consent
- Standard EU Contractual clauses

or

- Binding Corporate Rules (BCR)



8. International Personal Data Transfers (2/2)





8. International Personal Data Transfers (2/2)

Can personal data from the EU be transferred to and stored in the US with no guaranteed on an adequate level of data protection as required under the GDPR?

This was the central question in the Schrems II case before the CJEU. Ruling was issued on July 17, 2020



EU-US Personal Data Transfer framework

- 2013 → Austrian privacy activist Max Schrems filed a complaint with the Irish Data Protection Commission (DPC) against Facebook,
- U.S. authorities/ Access his PD/ violation 1995 DP Directive – Pre GDPR.
- 2015 → CJCE Safe Harbor framework → Invalid (*Schrems I*).
 - ✓ U.S. companies/ self-certify adherence to various privacy principles
 - ✓ U.S. authorities had access to the personal data of EEA-based individuals/ Edward Snowden.



Consequences/ Impact

- EU/U.S → Safe Harbor replaced by SH Privacy Shield
 - ✓ a Privacy Shield sought to address the issues the CJEU
 - ✓ Self certification remained the same;
 - ✓ After *Schrems I*, Facebook decided to rely on the European Commission-approved SCCs as the data transfer mechanism by which to transfer personal data to the U.S.
 - ✓ SCCs are approved data contracts that two parties can enter into to transfer data from the EEA to other countries.



Schrems' reactions

- 2015 Schrems submitted another complaint to the Irish DPC, relying on similar arguments to those made in *Schrems I*
- Alleging that the SCCs are also inadequate.
- *Schrems II* addressed both the SCCs and the Privacy Shield.



Privacy Shield

- Not a valid mechanism for transferring PD to the US
 - ✓ limitations on the protection of PD under U.S. law,
 - ✓ disproportionate access and use of EEA personal data by U.S. authorities with no effective redress mechanism for data subjects.
 - ✓ In particular, the access to PD under U.S. surveillance programs NOT limited to what is “strictly necessary,”
 - ✓ Privacy Shield also does not grant individuals based in the EEA actionable rights before U.S. courts against U.S. authorities.
 - ✓ Privacy Shield therefore cannot ensure a level of protection essentially equivalent to that arising from the GDPR as supplemented by national data protection laws across EEA countries

SCCs

- SCCs → provide sufficient protection for EEA personal data.
- Data Exporter ensure an adequate level of data protection is provided in the country where the data importer is based:
- Controller/Processor/ verify/ third country/adequate protection, under EU law.
- If so, CJCE → “additional safeguards” to those offered by the SCCs, but it did not elaborate on the form such safeguards could take.
- Data Protection Directive 1995. The CJEU did not comment on the need for the SCCs to be updated for alignment purposes with GDPR requirements.



Key Takeaways

- If an organization's data transfers from the to the U.S. are currently based on the Privacy Shield, it should begin to consider alternative data transfer mechanisms.
- EU got plan to Privacy Shield pitfalls is already underway.
- If relying on SCCs
 - ✓ Due Diligence procedures to assess compliance with GDPR
 - ✓ It remains unclear what would happen if different organizations drew different conclusions about what constituted adequate compliance.



9. Outsourcing in the Financial Sector

Circular or guidelines from the National Competent Authority (NCA)

- Data protection shall be guaranteed at all times
- Pay attention to data protection provisions in case of outsourcing of services including client or employee data
- Check if notification to the NCA is required
- Check which counterparts including sub-contractors or service providers are involved and in which jurisdiction
- The outsourcing does not relieve the institution of its legal and regulatory obligations or its responsibilities to its customers.
- The outsourcing shall not result in any delegation of the institution' responsibility to the subcontractor



10. Data Breach Management (1/2)



Data Breach : A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service

- Examples of data breaches

All sorts of accidents such as:

- A third person gets access to servers containing customer data through the internet due to security breaches in the computer system of the service provider
- At some point, everyone can access to online client accounts without passwords while only a client with a password should have access to his account
- An employee of a service provider loses a CD, an USB stick, a smartphone with customer data on it
- A commercial agent of a mobile operator in a shop loses a contract from a new customer



10. Data Breach Management (2/2)

- What to do in case of breach ?
 - Notify the DPA within 72 hours (under GDPR)
 - If personal data or privacy data are affected => notify the data subject without undue delay

- Inventory of personal data breaches to be maintained (registry)

- Some exemptions from the obligation to notify (risk assessment from a data subject perspective)



11. Sanctions – Fines and Penalties

- The GDPR imposes fines on data controllers and processors for non-compliance
- Under GDPR, processing of personal data without observing the required formalities provided by law is punishable by :

**finer up to €20 million
or
2%-4% of the worldwide annual revenue of the prior financial
year, whichever is higher**

(nature of infringement, intention, mitigation, preventative measures, history, cooperation, data type, notification, certification, other...)



12. Enforcement Actions



NHS Trust fined £325,000 following data breach affecting thousands of patients and staff

October 2010

Discovery of highly sensitive personal data belonging to tens of thousands of patients and staff – including some relating to HIV - on hard drives sold on an Internet auction site.

June 2012

The ICO announces that NHS Trust has been served with a civil monetary **penalty of £325,000 following** a serious breach of the Data Protection Act.



Google gets record fine of \$22.5 million over FTC charge of Safari tracking

2011

Google **implements a tracking cookie on users of Apple's Safari Internet browser** in iPads, iPhones and Macs, by circumventing Safari's default cookie-blocking setting.

August 2012

The Federal Trade Commission imposes a **fine of \$ 22,5 million** to Google. This is the largest penalty against a company for violating a privacy agreement in the USA.



CNIL issues a warning to ACADOMIA for excessive comments in its files

November 2009

The CNIL conducted an on-site inspection of ACADOMIA, a company specialising in home study courses.

CNIL identified the **presence of excessive and abusive comments** towards identified teachers, parents and students, such as “fat pig”, “f**** kid”, “cancer lung much deserved” or “the father is in prison”.

April 2012

Regarding the number of deficiencies found and their severity, CNIL addresses a public warning to ACADOMIA and informed the Prosecutor of the violations that may constitute criminal offenses.



Groupon in India notifies a data breach to its customers

January 2011:

Groupon was alerted of a security issue potentially affecting subscribers of Sosasta, a website acquired by Groupon in January 2011. Groupon corrected the problem, notified the breach to the concerned subscribers and advised them to change their passwords.

Following the data breach, Groupon reviewed the security procedures for Sosasta and implemented measures designed to prevent this kind of issue from recurring.





13. Practical Cases

Rights of the Data Subject

- A client complains because he has received marketing advertisements on his personal email
- You are the Data Protection Officer

➤ ***How do you handle the situation?***



13. Practical Cases

Right to be Forgotten

- A client wants to close his bank account and requests to :
 - receive all data which has been collected by the Bank
 - the Bank to delete all this data
 - You are the Data Protection Officer
- ***How do you manage these requests ?***



13. Practical Cases

Transfer of Data

- Your Bank has different branches worldwide, based in EU, USA and Asia
 - Each branch has its own HR software
 - In order to improve the HR processes, the Bank wants to change its HR software and to set up an unique solution which will be hosted in India and managed in Luxembourg
 - You are the Data Protection Officer
- ***What would be your approach?***



13. Practical Cases

Regulated data

- You are the Data Protection Officer of a Bank based in Luxembourg
 - Your Bank wants to launch a new product which is health insurance
- ***What measures would you take from a data protection point of view?***

Additional case Studies







Warning

The knowledge provided by this document is purely informative. Although the House of Training does its utmost to ensure that this information is correct and up to date, it disclaims any responsibility as to possible damages, losses, loss of earnings, direct or indirect.

The contents are subject to the laws of copyright, all rights reserved.