COMBATING MONEY LAUNDERING, THE FINANCING OF TERRORISM AND
THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION AND CORRUPTION

SPECIAL PRACTICAL GUIDE **#2**

BUSINESS RISK ASSESSMENT

AMSF
MONEGASQUE FINANCIAL SECURITY AUTHORITY

ORDRE DES AVOCATS DE LA PRINCIPAUTÉ DE MONACO

CONTENTS

This Special Practical Guide is proposed by the AMSF and the Conseil de l'Ordre des Avocats (Bar Council) in order to provide operational and concrete support to all financial institutions (FIs) and designated non-financial businesses and professions (DNFBPs), subject to Act 1.362 as amended, in the implementation of their system for combating money laundering, the financing of terrorism and the proliferation of weapons of mass destruction and corruption (AML/CTF-P-C).

Act 1.362 of 3 August 2009 requires persons subject to the legislation to implement a risk-based approach and makes it compulsory to carry out business risk assessment at entity level (see Art. 3 of Act 1.362, as amended)

This Practical Guide is for information purposes only. The only authoritative texts are the laws and regulations governing the AML/CTF-P-C system in Monaco. It does not cover all the obligations and the details of these obligations: the application of the measures presented in this Practical Guide alone does not guarantee that the Supervised entity complies fully with the legal obligations in force. For more information, please refer to the Generic Guidelines, which are regularly updated.

Each reporting entity shall be responsible for compliance with the legal and regulatory obligations in force, according to the risks specific to each entity.

This guide takes account of the regulations in force on 30 September 2023.

CONTEXT

Supervised entities are legally required to have an adequate level of understanding of the AML/CTF-P-C risks to which they are exposed. This is an essential prerequisite for the application of a risk-based prevention system.

Having a well-documented global business risk assessment enables the Supervised entity to effectively fulfil its AML/CTF-P-C obligations by allocating its resources appropriately.

Those subject to AML/CTF-P-C obligations are required to be aware of the risks in this area on two levels:

- at the level of their **establishment** (or overall risk assessment), with the aim of identifying the risks to which their business exposes them and defining an AML/CTF-P-C system that is adapted and proportionate to these risks;

- at the level of each customer* with whom they carry out an occasional transaction* or establish a business relationship*, in order to identify the specific risks associated with that customer and thus adapt the due diligence measures to be applied.

Only the business risk assessment is presented in this practical guide.
This is a multi-stage process consisting of:

- **identifying and understanding the ML/CTF-P-C risks** to which the business is exposed;

- **determining whether risks are mitigated** by internal controls and procedures;

- and finally establishing the residual risk*.

(1) Art. 3 of Law No. 1.362 amended
** Refer to the glossary on page 30*

WHAT IS A BUSINESS RISK ASSESSMENT?

A comprehensive risk assessment is the process by which supervised entities identify the threats* to which they are exposed and their vulnerabilities* to these threats, and then assessing the likelihood and impact of ML/CTF-P-C risks on the business.

This assessment forms the basis on which an entity is able to determine the areas to be prioritised in terms of AML/CTF-P-C and to ensure that the measures taken, the policies, procedures and controls in place are proportionate to the risks identified.

A properly conducted businessl risk assessment is therefore the foundation of the risk-based approach. Act 1.362 requires supervised entities to "apply appropriate vigilance measures, which are proportionate to their nature and size to meet the obligations set out in this Act, based on their assessment of the risks presented by their businesses in terms of money laundering, terrorist financing and the proliferation of weapons of mass destruction and corruption" (Art. 3, Act 1.362 of 3 August 2009, amended).

The risk-based approach is therefore based on two consecutive elements:

- understanding the risks faced by a reporting entity;

- implementing controls, policies and procedures to reduce the risks identified.

> "Reporting entities must ensure that their overall assessment is adapted to their business profile and takes into account the factors and risks specific to their activity.

** Refer to the glossary on page 30*

POINTS TO WATCH

A generic risk assessment that has not been adapted to the supervised entity's specific needs or business model will not meet the expectations of the AMSF or the Conseil de l'Ordre des Avocats (Bar Council).

Supervised entities **belonging to a group** must also carry out their own individual assessment, and not rely solely on the business risk assessment of the group.

GOOD TO KNOW

A list of general risks is available in the Generic Guidelines (Click here to access the Generic Guidelines).

This list of risks is not exhaustive and must be considered and adapted to suit your own entity, based on your knowledge and experience.

YOUR RESPONSIBILITIES

The supervised entity's business risk assessment must meet a number of conditions if it is to comply with the obligations set out in the legislation. There are 3 types of conditions to consider:

Formal conditions

- The assessment must **be documented**, to provide evidence that an appropriate analysis has been carried out. All sources of information used must be specified;
- **Its methodology must be described** and explained. It must specify the reasons why the reporting entity considers a level of risk (low, medium or high) for each factor;
- The assessment must conclude with **a result** that corresponds to the entity's overall risk level;
- The assessment must be **sent to the supervisor** on request (AMSF or Conseil de l'Ordre des Avocats (Bar Council), depending on the profession).

The conditions for its development:

- The assessment must be specific to the supervised entity's activity, i.e. proportionate to the nature and size of the business;
- It must involve a number of people, in particular those responsible for the AML/CTF-P-C functions, internal audit (if it exists) and all staff involved in activities relating to AML/CTF-P-C measures, the controls carried out in this context and the drafting of internal procedures;
- It must include an analysis of the inherent risks* taking into account risk factors*. These inherent risks correspond to structural risks (nature of the activities carried out, product lines, markets, etc.), risks linked to business data (customers, geography, distribution channels, etc.) and other risks (new products, outsourcing, etc.);
- It must present the risk mitigation measures (i.e. the measures and means included in its procedures) and estimate the extent to which the risks are covered according to the following logic:

** Refer to the glossary on page 30*

Conditions for validation and updating

- It must clearly **differentiate** between the risks of money laundering and the risks of terrorist financing;
- It must take into account the results of **Monaco's National Risk Assessment**, country risk analyses, sector risk analyses published or communicated by the supervisor and any other relevant source of information;

For your information, the results of the National Risk Assessment are published on the AMSF website.

- It must **be approved in a written document by the entity's management** or top management;
- It must be **regularly updated and reviewed**, either when there are changes in the factors listed above, or on a regular basis to ensure that the conditions in which the company operates have not changed significantly;
- It must take into account the results of Monaco's National Risk Assessment.

POINTS TO WATCH

A business risk assessment must be a "living" tool. It should enable the reporting entity to monitor the risks of its business and adjust the AML/CTF-P-C resources deployed.

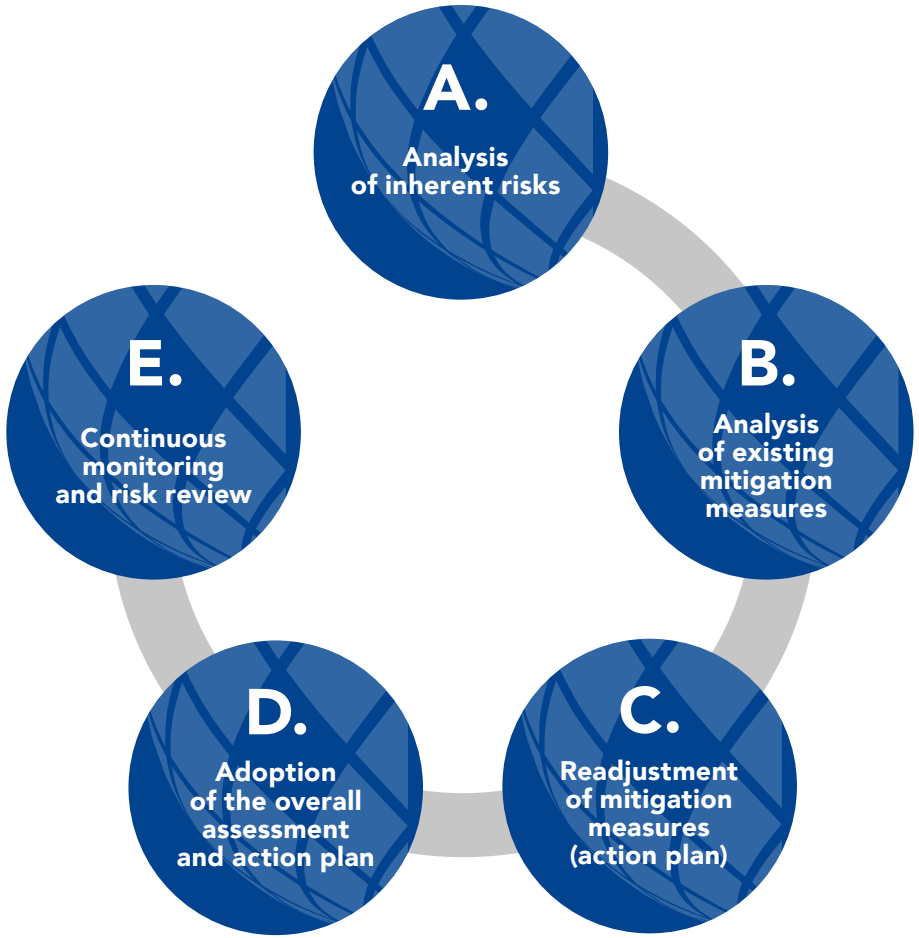
e.g.: a fast-growing business with changing characteristics (customers, transaction methods, distribution channels, etc.) risks having an obsolete AML/CTF-P-C system. The solution will therefore be to strengthen it to counter the main risk factors that have evolved.

WHAT DO YOU NEED TO DO?

How do you carry out a business risk assessment?

A business risk assessment requires a good understanding of the ML/TF-P-C risks to which a reporting entity is exposed.

There is no standard methodology common to all professionals for business risk assessment. However, the business assessment must include **the following 5 stages:**



A. ANALYSIS OF INHERENT RISKS

Inherent risk is the risk to which the supervised entity is exposed prior to the adoption of any policy, procedure, control or mitigation measure. This is the initial or theoretical risk associated with the activity.

It is determined by taking into account various **risk factors**. Professionals must take into account **at least the 5 risk categories** mentioned in Article 3 of Act 1.362 (customers, products and services offered, geographical areas, distribution channels, transactional activities).

POINTS TO WATCH

It is important to note that risk factors are not static. A reporting entity may have to take into account additional or new risk factors over time. It is inevitable that the environment in which supervised entities conduct their respective activities, as well as their relationships with their clients, will evolve, leading to the emergence of risk factors that were not previously taken into account.

For each risk category, several variables must be taken into account which, either alone or in combination with others, may increase or decrease the ML/TF-P-C risk posed to a supervised entity.

Therefore, for each **risk factor**, a supervised entity must :

- **Identify the ML/TF-P-C risks**;
- **Evaluate the probability that they will materialise**;
- **Measure their potential impact on the supervised entity**.

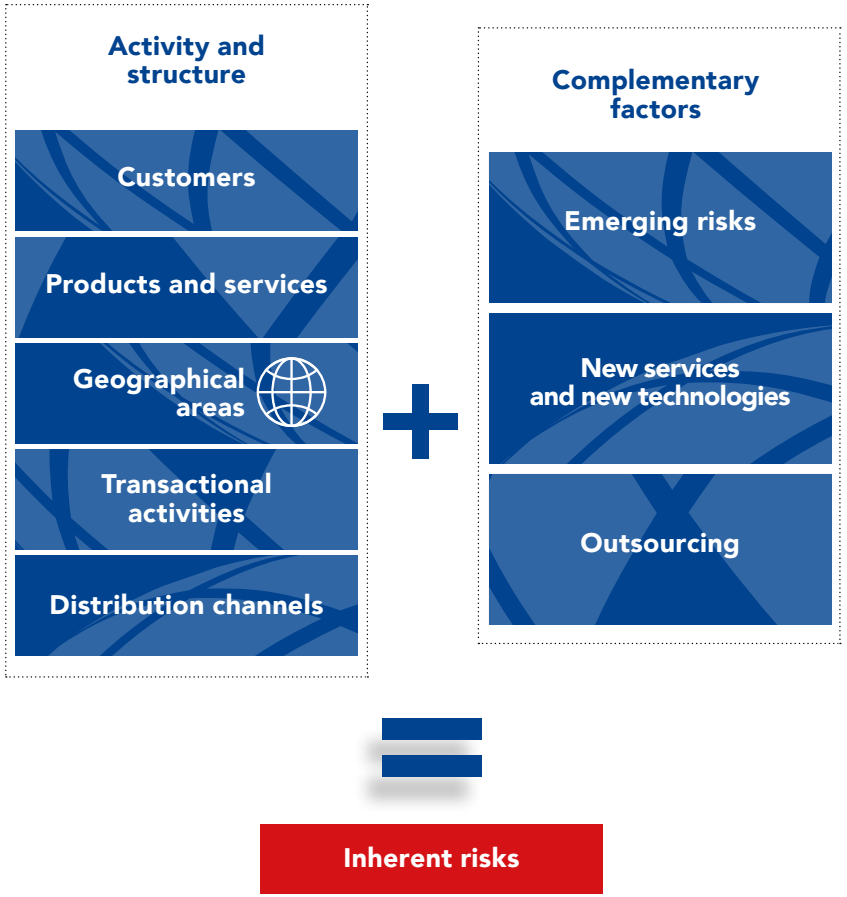
The impact consists of the nature and severity of the harmful result and can take several forms: reputational risk, business risk, regulatory risk, legal risk, financial loss, etc.

The likelihood of the risk materialising and **its impact** determine the level of inherent risk to which a reporting entity is exposed for a particular factor. The sum of the inherent risks represented by each factor corresponds to **the entity's inherent ML/TF-P-C risk**.

POINTS TO WATCH

The sources of information used should include quantitative and qualitative data - for example: types and number of customers, volume of transactions by type of customer, volume of business by type of product and service and geographical factors (see following pages).

To carry out a business risk assessment, the sets of inherent risk factors to be taken into account include (see appendix: operational examples of risk factors)



Structural factors

Structural factors correspond to a supervised entity's "macro" data (essentially accounting data as well as all other figures derived from the business), in particular:

- the size of the business;
- the form in which it is incorporated;
- the activity carried out;
- the competitive environment;
- number of employees, etc.

The size of the entity automatically determines the proportion of resources it will have to devote to its AML/CTF-P-C system.

Customer risk factors

Before entering a business relationship, in particular, the nature of the customer base (legal or natural persons, trusts, legal arrangements), the characteristics of certain customers (politically exposed persons, reputation) and the volume of business represented by the customer base, the length of the business relationship, the existence of targeted financial sanctions must be taken into account.

Examples of increased risk factors:

a. The business involves cash;
b. The activity is generally associated with a higher risk of corruption (for example, the arms trade, the defence industry and the mining industry);
c. The activity is associated with a higher risk of ML/TF-P-C (e.g. virtual assets and money transfers);
d. The business is conducted through opaque and complex structures for which there seems to be no legitimate justification.

On the other hand, certain characteristics may lead us to consider that the risk is reduced:

a. The activity does not involve the use of cash or crypto-currencies;
b. The business is conducted solely with a customer who is part of the same group;
c. The client is a company listed on a regulated market.

POINTS TO WATCH

In addition to the customer's activity, other factors may lead the customer to be considered as presenting a higher ML/TF-P-C risk, for example when the persons involved in the activity include PEPs or persons entrusted with an important function by an international organisation.

Risk factors relating to products, services and transactions

Product, service or transaction risk is the risk to which a reporting entity is exposed as a result of providing a particular product or service, or carrying out a particular transaction.

This risk depends on quantitative and qualitative factors.

Examples of quantitative factors:

- The number of products, services and transactions;
- The number of customers for each product and service;
- Business volume (sales) by product and service;
- The duration over which the transaction is carried out.

For each product, the qualitative risk factors that characterise it must be taken into account. For example, the following may be taken into account.

The level of transparency or opacity offered by the product, service or transaction

Products or services which, by their nature, allow or facilitate the anonymity of the customer or beneficial owner or facilitate the concealment of their identity, must be considered as presenting a higher ML/TF-P-C risk than other products or services.

For example, products such as mandate or omnibus accounts, as well as fiduciary services, present a low level of transparency and therefore a high level of risk.

POINTS TO WATCH

The ability of a third party to give instructions, even if it is not a party to the commercial relationship, must also be taken into account.

The complexity of the product, service or transaction

The risk presented by a product or service is determined by **the complexity of the transactions that can be carried out using it**.

A product or service used to carry out international transactions involving several parties and several countries must be considered as presenting a higher risk than a product or service used to carry out regular transactions involving constant amounts, and whose source is known.

For example, an account intended solely for salaries in a company does not present any particular risk.

The value and/or size of the product, service or transaction

It must be determined whether the product or service enables **high-value transactions** to be carried out. A payment instrument or account without any limits or caps presents a higher risk than a similar instrument or account that does not apply the same, although the level of these limits or caps must be taken into account.

A product or service that requires **a lot of cash** must be considered as presenting a higher risk than other products that cannot be financed in this way.

Supervised entities must be vigilant about the payment and/or financing methods offered. For example, cash, prepaid cards and virtual assets.

Risk factors relating to distribution channels

The distribution channel may constitute a risk depending on the way in which the supervised entity interacts with the customer.

Here are some examples:
- The number of business relationships initiated on a non-face-to-face basis;
- The number of distributors and agents marketing the product/service;
- The number of customers introduced by business introducers and intermediaries;

GOOD TO KNOW

Interacting with non-face-to-face customers should not necessarily be considered as automatically presenting a high risk of ML/TF-P-C.
The implementation by the superivsed entity of technological means within its systems to deal with the risk of identity theft or identity fraud would considerably reduce the inherent risk arising from this form of interaction with customers. In the absence of such systems, the risk must always be considered high.

Where customer relationships are conducted through several levels of **intermediaries**, supervised entities must take into account the reliability of these intermediaries and the AML/CTF-P-C standards to which they are subject.

The same applies when a customer is recommended by a **business introducer** or another entity forming part of the same entity.

Facteurs de risque liés à la zone géographique

The **geographical risk** arises from links with certain countries presenting a higher risk of ML/TF-P-C. To assess this risk, it is necessary to identify where:

- the customer or the beneficial owner is based;
- the principal place of business or activity generating the customer's or beneficial owner's assets.

Account should also be taken of the risk arising from countries with which the customer has commercial, financial or personal links.

The criteria to be taken into consideration are:

- countries on the European Commission's list of third countries with strategic deficiencies in their AML/CTF regime;
- countries identified by other credible sources as having serious deficiencies in their AML/CTF framework (e.g. FATF, MONEYVAL, IMF, etc.);
- countries subject to sanctions, embargoes or similar measures issued by international organisations such as the United Nations Security Council or the European Union. In addition, in certain circumstances, it is advisable to take into account countries subject to sanctions or measures from other lists (e.g. OFAC sanctions);
- countries providing funding or support for terrorist activities or in which terrorist organisations operate, identified by credible sources;
- countries identified as having significant levels of corruption or other criminal activity through credible sources, such as Transparency International's Corruption Perceptions Index;
- countries that have shown a lack of willingness to comply with international standards of tax transparency and information sharing (for example, non-compliance with or application of the common reporting standard);
- countries that fail to implement effective measures to ensure transparency and availability of information on beneficial owners.

POINTS TO WATCH

Membership to regional or international bodies such as the FATF and MONEYVAL, along with not being identified by a black or grey list, do not necessarily mean that the country presents a low ML/TF risk.
This may mean that a country has not yet been assessed by an international organisation, or that the shortcomings identified during an assessment were not sufficient to warrant listing.
These failures must be taken into account when they constitute relevant data for the supervised entity.

Risk factor linked to the technologies used

The legal framework requires supervised entities to identify and assess the ML/TF-P-C risks that may arise from
"the development of new products and new commercial practices, including new distribution mechanisms and the use of new or developing technologies in connection with new products or pre-existing products".

Other risk factors

The risk factors presented in this guide are not exhaustive. Therefore, depending on the complexity of the business and the variety of different risk factors for a particular business or entity, certain additional risk factors need to be taken into account.

Example: outsourcing, i.e. delegating the implementation of parts of its AML/CTF-P-C measures, policies, controls and procedures to a third-party service provider. Outsourcing introduces an additional variable, since the reporting entity will be dependent on the reliability and quality of the service provider's work to obtain the necessary information on which to base its decisions, including information that may influence its business risk assessment and the changes made to it.

POINTS TO WATCH

The assessment of "inherent risks" requires supervised entities to define weighting coefficients for the various risk factors. This weighting puts the importance of each factor into perspective.

There is no **standardised method** for defining these weighting coefficients, but supervised entities must take into account the relevance of the various risk factors in the context of their business.

In this context, reporting entities should ensure that:
- A factor is not overweighted;
- Economic or commercial considerations do not influence the weighting;
- The weighting does not allow a high risk factor to be underestimated;
- Situations where legislation considers risk factors to be increased should not be assigned an underestimated level of risk;
- Supervised entities should be able to "control" the calculated level of risk, or such a decision should be properly justified and documented.

In addition, if the supervised entity uses an automated risk scoring system that was not designed in-house but acquired from an external supplier, the supervised entity should ensure:
- That it fully understands the scoring methodology developed by the supplier and how the risk factors are combined to obtain the overall level of inherent risk;
- That this methodology complies with the legislative and regulatory obligations to which the entity is subject and that the estimated risks are consistent with the entity's understanding of its risks.

B. ASSESSMENT OF THE NATURE AND INTENSITY OF MITIGATION MEASURES IN PLACE

The level of inherent ML/TF-P-C risk, which corresponds to the accumulation of the risk factors identified above, has a direct impact on the type and level of the entity's AML/CTF-P-C resources. This level makes it possible to identify the areas where existing measures need to be strengthened or even reinforced.

> "To assess the effectiveness of the measures, policies, controls and procedures in place, the level of residual risk must be examined.

Once a supervised entity has identified the inherent ML/TF-P-C risks to which it is exposed, it must adopt measures, policies, controls and procedures either to prevent these risks from materialising or to mitigate their occurrence.

Measures, policies, controls and procedures must include:

- **customer due diligence**, record-keeping and reporting procedures;

- risk management measures, including **customer acceptance policies**, global customer risk assessment procedures, internal control, compliance management, communications and employee selection policies and procedures.

Their effectiveness will depend on their application in the day-to-day operations of the entity concerned. It is therefore essential to constantly monitor the way in which they are applied. This monitoring will enable the reporting entity to ensure that they are applied correctly, to determine their effectiveness and to identify and remedy any shortcomings in good time. In addition, through this monitoring, additional risks may be identified that could contribute to further strengthening the institution's l AML/CTF-P-C risk assessment.

GOOD TO KNOW

it is not necessarily mandatory to set up an internal audit function to provide this oversight. An external consultant may be hired to assess the adequacy of internal controls, policies and procedures. If this task is carried out internally, it may be entrusted to a person other than the Compliance Officer or any other person involved in the implementation or operation of the AML/CTF-P-C. Compliance Programme

C. FORMULATING A RESPONSE TO THE RISK

Any remaining risk is referred to as "residual risk". Whatever measures, policies, controls and procedures are adopted, there will always be a level of ML/TF-P-C risk that cannot be managed, avoided or controlled.

At this stage, once established, the supervised entity is required to check whether the residual risk is in line with its risk appetite, i.e. the level of risk it is prepared to assume.

For example, an institution that has customers in a country that presents AML/CTF-P-C risks should consider the need to acquire specialized search engines for that jurisdiction, or even to expand its compliance function by adding a new employee from that jurisdiction.

Indeed, if revenue generated by these customers is growing, the establishment must ask itself what risk it is prepared to assume by not developing the means to deal with this risk.

More broadly, the supervised entity must determine the controls and mitigation strategies to be implemented. These are broken down into:

- an increase in resources;
- the introduction of new controls (in response to the emergence of new risks, for example);
- strengthening of existing controls: when it appears that certain risks are increasing, it may be necessary to modify the risk classification of customers for example.

D. ADOPTION OF A BUSINESS RISK ASSESSMENT

In principle, the business risk assessment must be carried out by each company **prior to starting its activity**.

The business risk assessment and action plan must be formalised in a written document (paper or digital). This document must be approved by a senior manager and made available to the AMSF or the Conseil de l'Ordre des avocats (Bar Council).

It is also important that **employees are made aware of the results of this assessment**, for example through the ongoing AML/CTF-P-C training programme. This ensures that employees are aware of the principal risks to which the entity is exposed and that they can effectively execute the policies, procedures and controls determined by senior management to mitigate the risks.

E. RISK MONITORING AND REVIEW

Since ML/TF-P-C risks are constantly evolving, the business risk assessment is a **periodic process** that must be **reviewed regularly** and, in particular, whenever there are significant changes in the management and operations carried out (for example: change in business model, customer base, risk exposure, etc.). It is recommended that supervised entities draw up a **list of events triggering** an ad hoc review.

A supervised entity is therefore required to review and update its overall risk assessment whenever:

- **new threats and vulnerabilities are identified**. It is possible that, in the course of its activities, the supervised entity may become aware of risks that it did not take into account in its initial risk assessment. Information may also become available on the emergence of new threats exploiting certain vulnerabilities. Where an entity is aware that a new risk has arisen or an existing risk has increased, this should be reported in the overall risk assessment as soon as possible;

- **changes are made to its business model, structures or activities**. Many changes could require such a revision.

POINTS TO WATCH:

The overall risk assessment must be kept up to date. To do this, a timetable should be set for the next assessment to ensure that changing, new or emerging risks are taken into account. As with the initial assessment, the update must be documented and proportionate to the ML/TF-P-C risk. The business risk assessment should be reviewed at least once a year or when triggering factors occur (for example, the launch of a new product, the start of a business relationship in a new country and/or the use of a new technology).

OPERATIONAL EXAMPLES OF RISK FACTORS

These risk factors should be read in conjunction with the risks mentioned in the Generic Guidelines (pages 22 to 24).

Examples of structural factors

Examples of data that should be collected and evaluated	Relevant quantitative data
• Type of business; • Company size; • Diversity and complexity of the sector; • Diversity and complexity of the markets in which the entity operates.	• Annual sales; • Net profit for the year; • Number of employees; • Number of branches or offices; • Number of steps where the entity operates; • Number of business sectors in which the entity operates; • Balance sheet total, overall and by sector/market.

Facteurs de risque liés au client

Examples of data that should be collected and evaluated	Relevant quantitative data
• Total number of customers; • Type of customer (natural persons, legal entities, legal arrangements); • Non-resident customers; • PEP (foreign, national and international organisations; customers and customers' BOs); • High net worth individuals; • Cash-intensive business; • Legal arrangements; • NPOs; • Other high-risk companies and links with sectors generally associated with a higher level of ML/TF risk; • Corporate customers with nominee shareholders or nominee directors; • Persons acting as representatives/agents on behalf of the customer; • Customers with complex ownership structures; • Holders of bearer shares or other bearer negotiable securities;	• Number of customers (individuals, legal entities and legal arrangements in the categories mentioned); • Total number of transactions; • Total value of transactions; • Total number of assets under management.

Facteurs de risque liés au client

Examples of data that should be collected and evaluated	Relevant quantitative data
• Complexity of the product, service or transaction; • Level of transparency of the product, service or transaction and the extent to which the product, service or transaction could facilitate or enable anonymity or opacity of customer, ownership or beneficiary structures; • Cash payment services; • Deposits; • Electronic transfers; • Private banking/wealth management; • Credit cards; • Prepaid cards; • Trade finance transactions; • Means of payment: Cash, cheques, prepaid cards, virtual money, etc.	• Number of products issued; • Number of customers (natural person, legal entity, legal structure) by product/service; • Transaction value by product/service; • Number of transactions for each payment method; • Volume of funds transferred for each payment method; • Profile of customers using specific payment methods.

Examples of risk factors linked to distribution channels

Examples of data that should be collected and evaluated	Relevant quantitative data
• Examples of data that should be collected and evaluated • Direct customer integration; • Non-face-to-face customer integration (e.g. via the Internet, including Internet banking and mobile banking); • Internet banking; • Mobile banking services; • Use of introducers, intermediaries and/or agents; • Use of third parties for customer knowledge; • New and untested distribution channels.	• Number of face-to-face business relationships concluded; • Number of commercial relationships concluded outside face-to-face contact; • Number of customers (individuals, legal entities and legal arrangements) integrated via each delivery channel; • Number of introducers, intermediaries and/or agents; • Geographical location of introducers, intermediaries and/or agents; • Geographical location of third parties; • Profile of customers using each delivery channel.

Examples of geographical risk factors

Examples of data that should be collected and evaluated	Relevant quantitative data
• Countries subject to sanctions - TF and PF; • Countries on the FATF black/grey list; • Offshore jurisdictions; • Non-compliant tax jurisdictions; • Countries associated with a high level of corruption or organised crime;	Breakdown by country for • Customers (individuals, legal entities and legal arrangements); • Beneficial owners of customer companies; • Transactions (incoming and outgoing); • Products and services • Introducers, agents, etc.

Sources of information

As part of the business risk assessment, the supervised entity must take into account various sources of relevant information. These include:

- Monaco's National Assessment of Money Laundering and Terrorist Financing Risks (NAR);
- Any global assessment of thematic risks (e.g. legal entities and legal arrangements, global assessment of TF risks, global assessment of tax evasion risks, global assessment of NPO risks);
- Global sector risk assessments;
- National assessment of risks in other jurisdictions in which the reporting entity operates or customers are based;
- Communications issued by the FIU, AMSF or Conseil de l'Ordre des Avocats (Bar Council);
- Guidance documents and any other communication from the AMSF, the Bar or other competent supervisory authorities;
- Information from industry bodies or representatives;
- Information from international standards bodies and international organisations, mutual evaluation reports from other jurisdictions and typology reports;
- The supervised entity's knowledge and expertise;
- Any other credible and reliable source.

EXAMPLE OF A PRACTICAL CASE

A company in Monaco sells and buys new and used luxury watches. In order to carry out its business risk assessement, the company has drawn up a risk classification based on 5 pillars:

- the nature of the products or services offered;
- the proposed transaction conditions/payment methods;
- the distribution channels used;
- customer characteristics;
- countries and geographical areas;

Methodology used:

1. Supervised entities draw up a list of the risk factors associated with their own activities.
2. Depending on the extent of the risks to **its business**, the supervised entity weights each of the risks identified according to their seriousness, frequency of exposure and probability of occurrence;
3. The supervised entity **must respond** to these risks with mitigation measures that are commensurate with the importance of the risks identified;

The residual risk (inherent risk + mitigation measures) is ultimately the risk that the supervised entity is prepared to accept. Failure to do so means that stages 2 and 3 must be reassessed.

Determination of inherent risk:

Macro analysis

generic guidelines established by the AMSF and other documents issued by the FATF in order to refine its knowledge of its obligations and the sectoral risks associated with its business. It noted that the sector in which it operates presents **a moderately high level of risk** in the renewable energy sector, which indicates that it will have to implement significant AML/CTF-P-C measures.

Through **typology studies**, it has also observed that the luxury watch sector is favoured by certain criminal organisations (theft, handling stolen goods, swindling). This initial analysis enables the company to understand the type of risk inherent in its sector. This enables it to analyse the situation in greater depth.

Specific analysis of risk factors

Following the macro analysis, the company considers that the value of goods bought and sold constitutes a risk in itself. This risk is further heightened by the fact that there is a high risk of buying a second-hand watch that has been stolen. Its exposure to money laundering linked to **the nature of the products and services** offered means that the risks involved in buying and selling must be taken into account.

This risk is amplified by the fact that most of our customers are foreign and just passing through. Certain customers, through business introducers, sometimes offer watches well below market value in exchange for cash. While the majority of our customers are individuals, some of our foreign customers are legal entities, whether or not they work in the luxury watchmaking sector.

It also observed that in its field of activity, even wealthy customers can carry certain risks (politically exposed persons, professional activity in a risky sector, risk of international sanctions) and particularly when they are not well known to the company (visiting foreign customers, business introducers, beneficial owners hidden behind a foreign legal entity). As Monaco is home to a large number of nationalities and is a popular holiday destination, it is naturally destined to attract cosmopolitan customers.

Weighting of risk factors and calculation of inherent risk

The company must then implement a table or tool that summarizes and describes its risk factors. It must **estimate** the level (based in particular on the statistical data it holds). Finally, it must weigh them up and derive from them a level of inherent risk.

POINTS TO WATCH

The table below, which is a very simplified example, shows the logic of the exercise, applied to the case described. This is not a model proposed by the AMSF and the Conseil de l'Ordre des Avocats (Bar Council), but a presentation intended to illustrate the approach. It includes some of the factors described, but is not exhaustive.

La modélisation de cette démarche se présente comme suit :

#	A	B	C	D
Risk categories	Products and services	Products and services	Means of payment	Customers riks
Risk Factors	Watches purchase/ high amount	Watches sales /high amounts	Cash	Occasional customer
Description/ assessment	Risk that the watches were stolen ou linked to criminal activities	Risk that buyers use watch purchase to launder money	Risk that buyers use watch purchase to launder money	Risk of wrong /lack of KYC
Estimated level (1 to 5)	2	2	4	4
Justification	The watches purchased belong to recognized brands and are all traced. The risk of their origin is not zero but the risk of intermediaries must be considered as a priority.	A limited proportion of the watches we sale have a value greater than €10,000.	Some customers ask us to use cash or crypto assets to buy watches without having any real interest in the product itself.	80% of our customers are occasional and not residents.
Weighting (coefficient 1 to 3)	3	3	3	3
Weighted rating	6	6	12	12

#	E	F	G	
Risk categories	Customers riks	Distribution Channels	Geographical Areas	
Risk Factors	Obfuscation	Intermediaries	Persons subject to TFS	
Description/ assessment	Risk of wrong /lack of KYC	Risk of wrong /lack of KYC	Risk of wrong /lack of KYC	
Estimated level (1 to 5)	5	3	5	
Justification	We have some legal entities as clients	We use intermediaries in several significant sales.	Our Russian-speaking clientele has been growing since 2022 and offers cash payments in many cases.	
Weighting (coefficient 1 to 3)	1	3	3	**Total**
Weighted rating	5	9	15	**65**

In this example, if we take into account risk factors A to G, we arrive at **an inherent risk level of 65**. The maximum theoretical level is 105 (5x3 for 7 factors identified), which corresponds to a moderately high level of overall risk.

Mitigation measures

Analysis of these risk factors and the level of inherent risk means that the company must adopt a high level of Know Your Customer (KYC) to ensure that customers, both buyers and sellers, are not linked to criminal organisations. To do this, it carries out in-depth research (or even subscribes to a specialised research tool).

With regard to the specific point concerning Russian-speaking customers, in addition to the measures described above, it must systematically consult the Monegasque list of fund freezes. For companies, it has decided to do the same with regard to beneficial owners, once they have been duly identified.

As far as business introducers are concerned, it has decided to use only professionals with a reputation for reliability and whom it knows well.

In all cases, and after considering that it does not have the capacity to effectively identify customers by remote means, it has decided to meet all its customers in person.

With regard to means of payment that could facilitate transactions linked to risky individuals, it has decided not to enter into cryptocurrency transactions and to significantly limit the use of cash.

Similarly, it favours distribution channels that it controls and refuses to carry out complex or unusual transactions, or transactions with people or structures in high-risk countries or geographical areas, without first carrying out a specific assessment.

The impact of these measures may be summarised and a residual risk established:

#	Description /assessment	Weighted rating	Mitigation measure	Estimated impact of the mitigation (in %)	Calculated residual risk
A	Risk that the watches were stolen ou linked to criminal activities	6	Extensive KYC research, face-to-face customer meetings, limitation of cash payments, refusal of cryptocurrency payments.	50%	3
B	Risk that buyers use watch purchase to launder money	6			6

#	Description /assessment	Weighted rating	Mitigation measure	Estimated impact of the mitigation (in %)	Calculated residual risk
C	Risk that buyers use watch purchase to launder money	12	Limitation of cash payments, refusal of cryptocurrency payments.	70%	3,6
D	Risk of wrong/lack of KYC	12	Extensive KYC researchs.	50%	6
E	Risk of wrong/lack of KYC	5	Face-to-Face meetings for all customers, refusal of complex operations	60%	2
F	Risk of wrong/lack of KYC	9	Limited use of intermediaries (only recognized ones)	66%	3,1
G	Risk of wrong/lack of KYC	15	Systematic special examination and consultation of the Monegasque list	60%	6
		65		**Total residual Risk**	**30**

In this hypothetical case, the residual risk falls to 30, a moderately low level. This residual risk corresponds to the company's risk appetite. It would be possible to further reduce this level by, for example, refusing all use of intermediaries or all payment in cash, but this would be to the detriment of its business.

POINTS TO WATCH

As this is a very simplified model, it does not specify the justification for the impact of mitigation measures: this must be formalised and explained.

POINTS TO WATCH

While there are risks common to all supervised entities in every sector of activity, the response is necessarily different from one supervised entity to another. This is due in particular to the differences resulting from the supervised entities themselves but also from the objective data derived from the aforementioned risk classification (5 pillars). Each supervised entity must therefore carry out its own analysis based on its own data. It is quite possible for 2 supervised entities in the same sector to have different overall risk assessments. In all cases, the business risk assessment must be documented and must be able to be demonstrated throughout the various stages of its development.

FAQ

What is the purpose of a business risk assessment?

The business risk assessment is a tool that helps supervised entities to determine the extent of their needs in terms of controls and control resources. For example, a supervised entity with a high proportion of complex sales (legal entity customers in complex arrangements) with risky customers (e.g. PEPs) should consider the level of its AML/CTF-P-C system and/or its risk appetite.

Should an external service provider be used to carry out the business risk assessment of the establishment?

The choice of whether or not to use an external service provider should be considered from two angles:

- The complexity of the activities involved and the number of risk factors to be considered;
- In-house capacity to develop relevant analysis and maintain it over time.

In any case, the establishment must be able to understand the logic behind the analysis that may be carried out by an external service provider, and it must accept the results.

Great care should also be taken when implementing a "turnkey" solution: the difficulty lies above all in reasonably measuring the mitigating factors and assessing their real impact on the entity's level of residual risk.

Is there a business risk assessment model recommended by the AMSF and the Conseil de l'Ordre des Avocats (Bar Council)?

Each supervised entity must estimate its needs in this area and certain models that exist on the market may be relevant for certain entity sectors/sizes. However, it is perfectly possible for small and medium-sized supervised entities to carry out a reasonable assessment by taking into account only the reasonable risk factors that apply to them.

The most important thing is to have an enforceable, justified and documented methodology. In particular, it must enable changes in inherent risks to be detected over time, so that they can be mitigated by means of new measures or strengthened or modified procedures.

REMINDER OF THE LAW AND PENALTIES

The reference text which defines all the obligations relating to the overall assessment of risks of all those liable is Article 3 of Act 1.362 of 3 August 2009, as amended:

"The organisations and persons referred to in Articles 1 and 2 shall apply appropriate vigilance measures, which are proportionate to their nature and size to meet the obligations of this Chapter according to their assessment of the risks presented by their activities in terms of money laundering, terrorist financing and the proliferation of weapons of mass destruction and corruption.

To this end, they shall define and implement mechanisms for identifying, assessing and understanding the risks of money laundering, financing of terrorism and the proliferation of weapons of mass destruction or corruption to which they are exposed, as well as a policy adapted to these risks.

In particular, they shall develop a risk classification, depending on the nature of the products or services offered, the conditions of proposed transactions, the distribution channels used, the characteristics of clients, countries or geographical areas and the State or territory of origin or destination of the funds.

Pour l'identification et l'évaluation globale des risques de blanchiment de capitaux, de For the identification and assessment of the risks of money laundering, financing of terrorism and the proliferation of weapons of mass destruction and corruption, they shall take into account:

- factors inherent to clients, products, services, distribution channels, the development of new products and new commercial practices, including new distribution mechanisms and the use of new or developing technologies related to new products or pre-existing products as well as countries or geographical areas;
- documents, recommendations or declarations from reliable sources, such as international organisations specialising in countering money laundering, terrorist financing and the proliferation of weapons of massive destruction and corruption;
- the national risk assessment;
- guidelines established, as the case may be, by the Monegasque Financial Security Authority or by the Conseil de l'Ordre des Avocats (Bar Council).

They shall also include the risks identified by the Government and the competent authorities in their own risk assessment.

The organisations and persons referred to in Articles 1 and 2 shall take appropriate measures to manage and mitigate the risks associated with the activities, business practices and products they offer, including with regard to new technologies.

The organisations and persons referred to in Articles 1 and 2 are required to document these assessments in order to demonstrate the basis thereof by means of any useful document, keep them up-to-date and be able to transmit them to the department exercising the Monegasque Financial Security Authority's Supervisory Function or to the Conseil de l'Ordre des Avocats (Bar Council), as the case may be, by any written means.

The risk assessment and the related documents may be kept in a digital format, subject to compliance with the retention conditions in accordance with the regulations in force ".

The AMSF can impose two types of penalty:

- Those referred to in Article 64-7 of Act 1.362, which correspond to shortcomings in voluntary procedures: failure to transmit the overall risk assessment, the annual activity report, the procedures in French, the annual questionnaire, etc.

- Those referred to in Article 65-1 of the aforementioned law, which concern breaches observed during on-site inspections carried out by the AMSF.

Regarding the sanctions falling under the Council of the Order, they are referred to in articles 69-1 to 69-4 of Act No. 1.362 and apply in the event of breach (including simple) of obligations in the fight against money laundering and the financing of terrorism. They can be brought against the Lawyer as well as employed individuals, employees, or acting on behalf of the Lawyer, due to their personal involvement.

GLOSSARY

Some of the terms used in Act 1.362, as amended, to describe the obligations relating to the business risk assessment in an establishment require clarification, as set out below. Their aim is to standardise practices within the profession.

It is up to the professional to define precise criteria to distinguish the different terms covered by the law (occasional customer, business relationship, etc.) in its internal procedures.

Terms	Practical Guidelines	Non-exhaustive examples
Customer	It is up to each professional to determine, on the basis of each situation, who is its customer and who are the beneficiaries and/or agents in the transaction or business relationship. As a reminder, the customer can be: • An individual (regular or occasional customer), Monegasque resident or non-Monegasque resident; • A legal entity (SARL, SAM, SCI, SCS, etc.), a legal or similar entity (trust, foundation, etc.). The term customer refers to the natural person, legal person or legal entity represented by the estate agent subject to registration in the context of its transactions. When buying or selling a property, this is the party represented by the agent: the buyer and/or the seller When letting a property worth more than €10,000, these are the parties in contact with the agent, usually both the owner and the tenant.	✓ Person who commissioned the estate agent to purchase a property; ✓ Person who commissioned the estate agent to sell a property; ✓ Owner of a property who has instructed the estate agent to let a property in excess of €10,000; ✓ Tenant of a property let by an estate agent for more than €10,000
Business relationship	"Business relationship means a professional or commercial business relationship linked to [the reporting entity's 5] professional activities, and which, at the time the contact is established, is intended to be of a long-term nature." This includes cases where: • a contract is drawn up between the customer and the agent, covering successive transactions or creating ongoing obligations for the parties; • in the absence of a contract, a customer regularly requests the services of the estate agent to carry out several transactions, or a continuous transaction.	✓ A customer making a property purchase; ✓ A customer who carries out several transactions in the same year (sale/purchase/rental); ✓ A customer who gives the estate agent a mandate for a sale, purchase or rental in excess of €10,000; ✓ A customer who signs a lease for a rental of more than €10,000 (owner and/or tenant).
Occasional transactions	Occasional transactions are one-off transactions that are not long-term.	✓ When a customer makes a one-off purchase or sale without showing any intention of seeking the estate agent's services again
Residual risk	The residual risk is the risk that remains after the application of mitigation measures.	
Inherent risk	Inherent risk is the theoretical risk associated with the business. It can also be defined as the initial risk, before any control measures (internal control). It differs from residual risk, which is the risk remaining after the implementation of control measures (internal control).	

Terms	Practical Guidelines	Non-exhaustive examples
Vulnerability	Vulnerabilities include the factors that make it attractive to commit an offence and the related money laundering or terrorist financing transaction. They are inherent to the structural characteristics of a given country and its financial centre. They are also linked to the practices and characteristics of the products used in a given sector of activity.	
Threat	A threat is a person, a group of persons, an object or an activity likely to harm the banking and financial system. Generally speaking, this notion includes criminal organisations, networks of swindlers or fraudsters, corruption networks, terrorist groups and their facilitators, their funds and their past, present or future activities.	
Risk factors	Risk factors are variables which, alone or in combination, can increase or decrease the ML/TF risk posed by an individual business relationship or occasional transaction.	

LIST OF ALL GUIDELINES

The following guidelines are currently available:

- Generic guidelines (published on 22 July 2021): these set out all the legal obligations and explain them in summary form, enabling reporting entities to understand all the AML/CTF measures to be implemented

- Guidelines for members of the bar established by the president of the Bar council in accordance with the provisions of article 53-1 of Act n° 1.362 as amended of August 3, 2009 (published on October 18, 2021)

- Practical guide to yachting (published on 25 January 2022)

- Practical guide for sports agents (published on 25 January 2022)

- Practical guide for estate agents (published on 11 December 2023)

AMSF MONEGASQUE FINANCIAL SECURITY AUTHORITY

13 rue Émile de Loth
98000 MONACO

Tél. (+377) 98 98 42 22
Fax (+377) 98 98 42 24
www.amsf.mc

ORDRE DES AVOCATS DE LA PRINCIPAUTÉ DE MONACO

11, rue Notre Dame de Lorète
98000 MONACO

Tél. (+377) 97 77 23 32
Fax (+377) 97 77 23 34
www.avocats.mc