AML Tuesday's Session #10 on:

Conducting a Business Risk Assessment

April 16, 2024

Discussion Topics

01 Purpose and relevance of the BRA

02 BRA process, sources and phases

03 Practical examples for FIs (per sub-sector)

01 Purpose and relevance of the BRA

FATF International standards on combating ML and TF

Recommendation 1 & interpretive note:

- Countries should require financial institutions to identify, assess and take effective action to mitigate their money laundering, terrorist financing risks and proliferation financing risks.

Recommendation 10 & interpretive note:

- Financial institutions should determine the extent of CDD measures using a risk-based approach (RBA):
  - Where the risks are higher, FIs should be required to conduct enhanced CDD measures
  - Where the risks are lower, FIs could be allowed to conduct simplified CDD measures

FATF Guidance on implementing the RBA for FIs

Monegasque legal framework

- **Art. 3 of Law No. 1.362,** as amended, lies down the obligation for FIs to apply **appropriate vigilance measures according to their assessment of the risks presented by their activities** in terms of ML/FT-P-C.
- To this end, they shall **define and implement mechanisms for identifying, assessing and understanding the risks of ML, FT-P-C** to which they are exposed, as well as **a policy adapted to these risks.** In particular, they shall develop a risk classification and take appropriate measures to manage and mitigate their risks.
- Art. 3 further outlines the **categories of risk factors** and some main **sources** (e.g. NRA) to be taken into account in the risk identification and assessment.
- **Breaches of Art. 3 can be sanctioned** as per Art. 65 et seq. both at entity-level and at level of directors, employees, agents & persons acting on behalf of the entity based on personal involvement,

Recent AMSF Guidance on the BRA (February 2024)

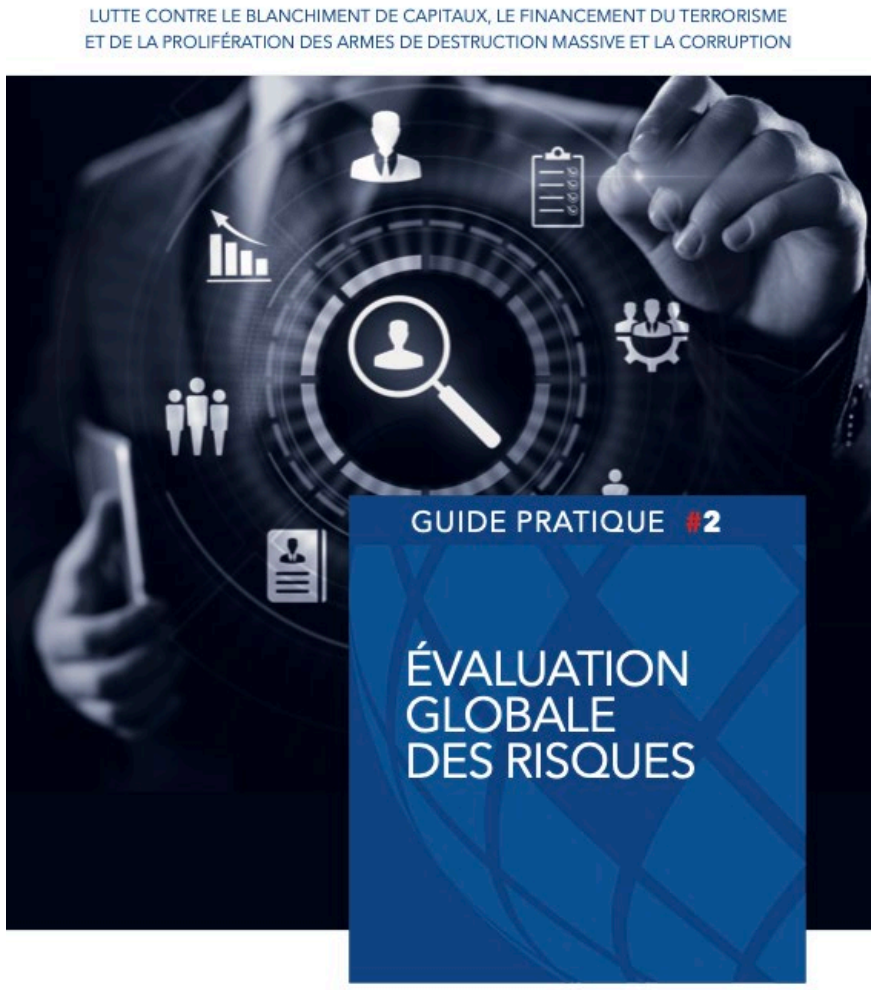


TABLE DES MATIÈRES

The difference between BRA and CRA

BRA

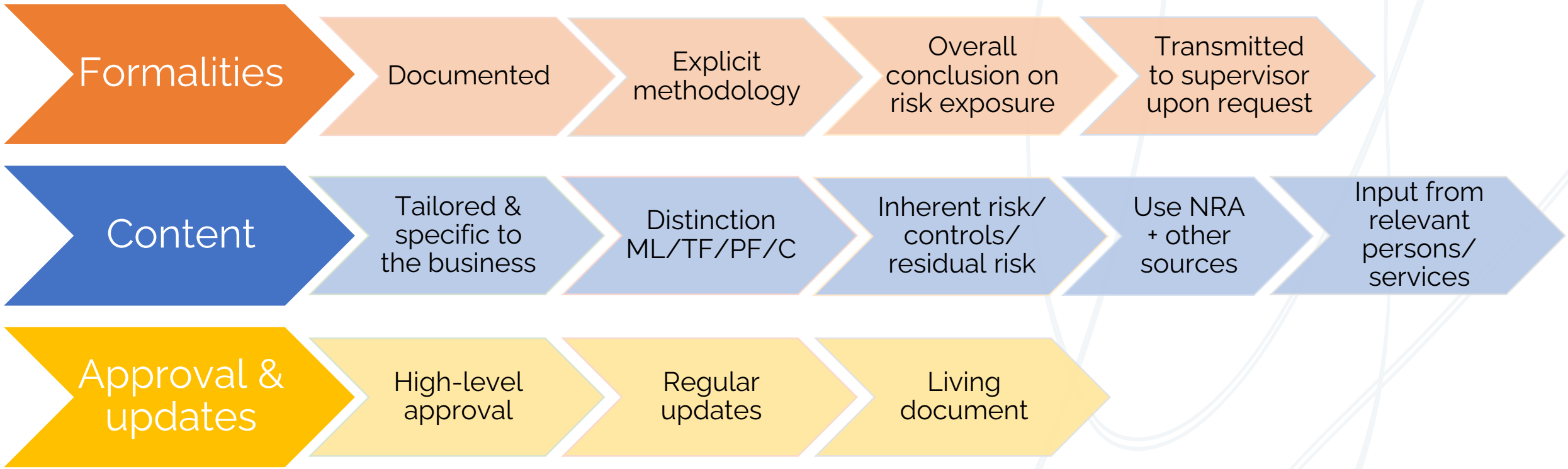
Identifies the risk of ML /FT-P-C posed to FI as a whole based on its activities

CRA

Assessment which specifically identifies the risks that each individual customer (private or corporate) pose to the business

02 BRA process, sources and phases

Requirements for development of BRA



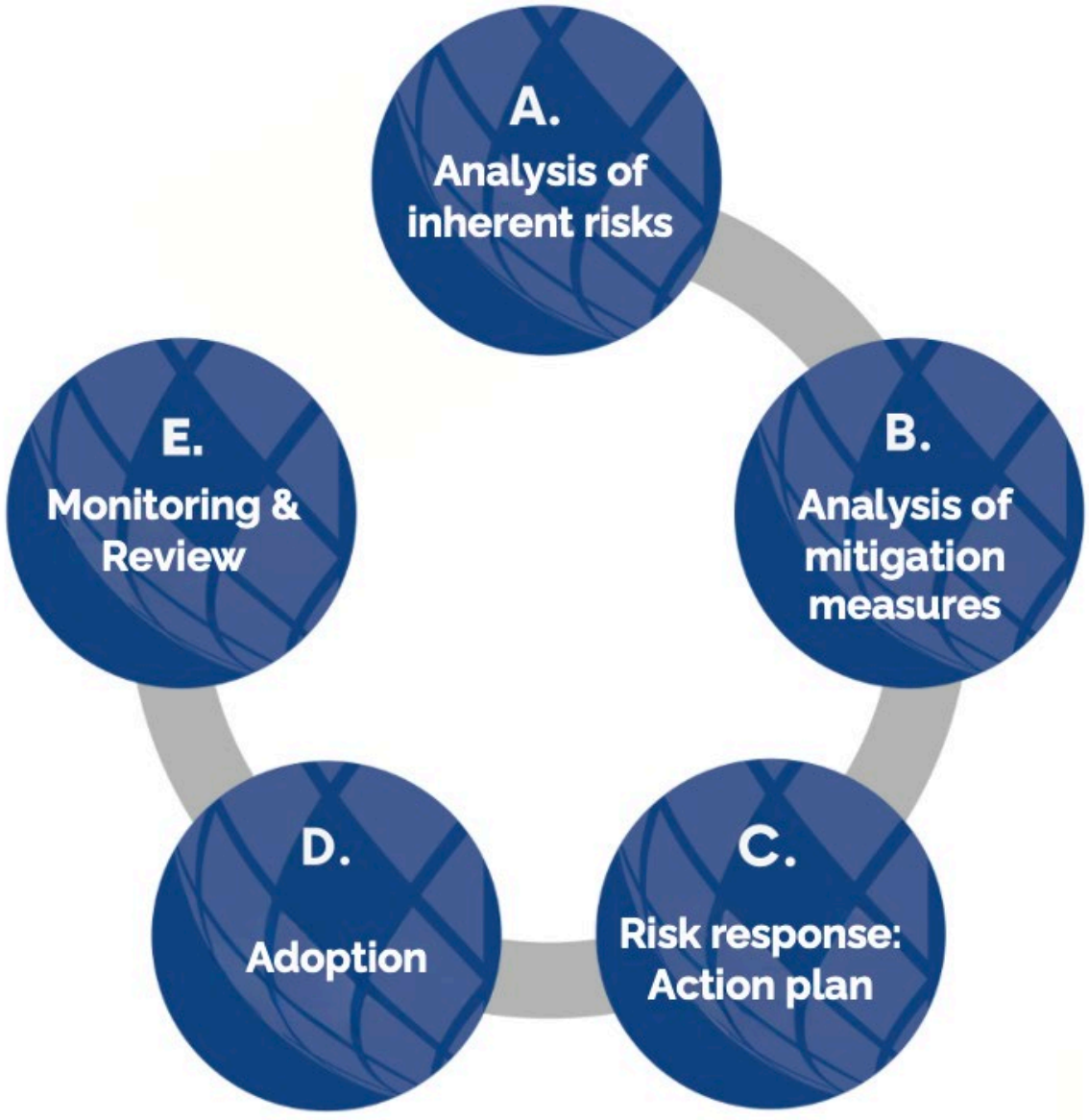
High-level external sources on risks

International guidance, typologies & evaluations	Information from professional sectorial bodies	Black lists, grey lists, sanctions lists
Topical risk assessments	**Monaco National Risk Assessment**	Sectorial risk assessments
(s)NRAs of other regions with links to the business	Communications by competent authorities	Guidance published by AMSF & Bar Association

BRA operational/internal sources - examples

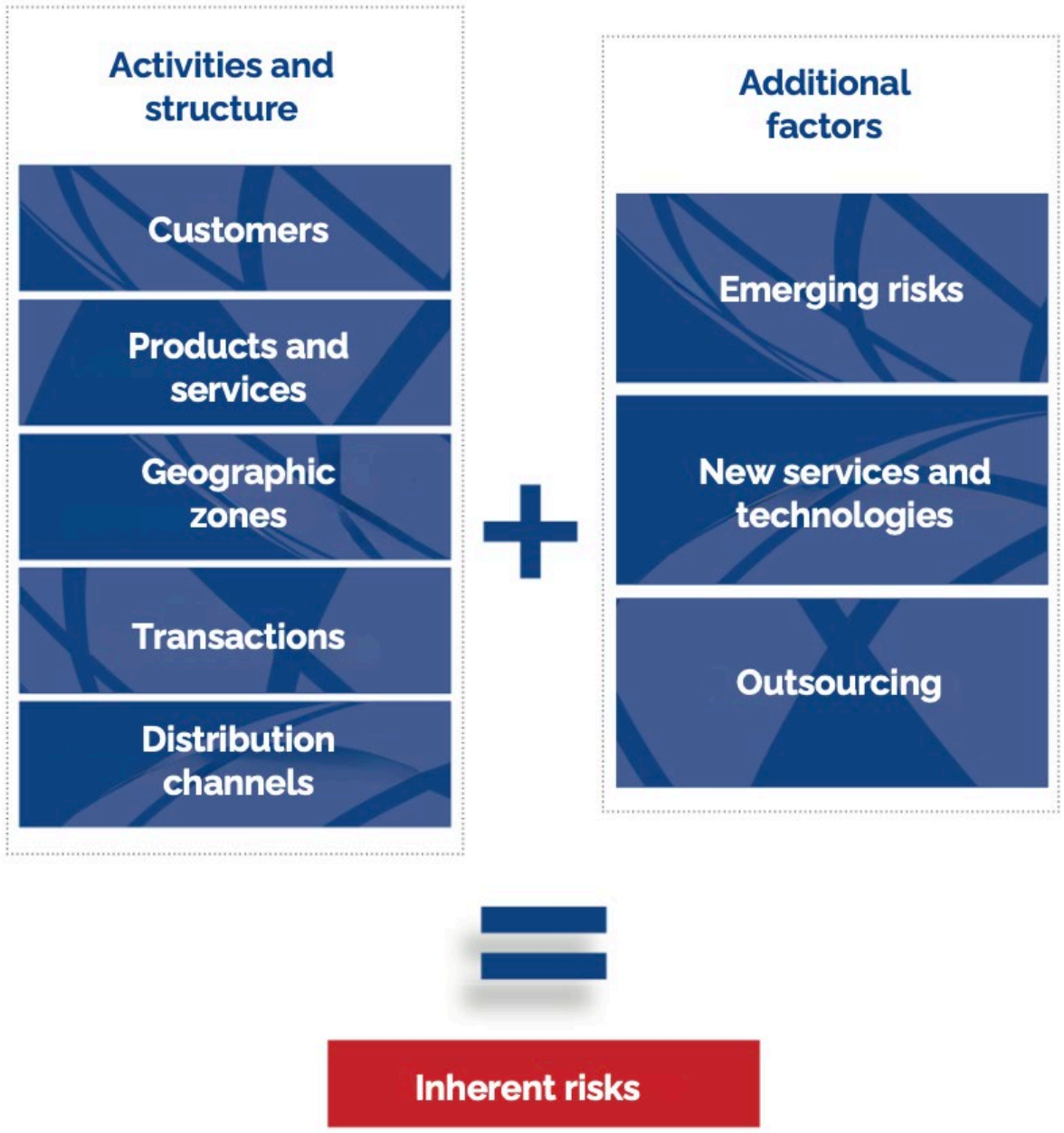
Data on customers: numbers, types, locations	Data on beneficial ownership of customers	Results of analyses of unusual & suspicious transactions	Findings of internal or external auditors
Volume of transactions	Proportion of cash transactions	Product range and characteristics	Reports from compliance
Exposure to certain industries/sectors	Size of the company	Use of third parties	Extent of non-face-to-face business

BRA phases



A. Analysis of inherent risks

- This phase relates to the **identification, assessment and understanding the inherent risks across the business**
- **Inherent risk** = the risk of ML/FT-P-C occurring without consideration of any controls or mitigant in place to alter the likelihood or impact of the risk
- For every risk factor, the FI must identify the **risks**, evaluate the **probability** that the risks will materialise and measure their potential **impact** on the business
- A **range of risk factors grouped under different categories** should be assessed – see next slide
- Data used should include up-to-date **quantitative and qualitative information**
- Risk factors should be **weighted depending on their relative importance** for the business. There is no one-size-fits-all method for this. The AMSF guidance sets out considerations to be taken into account by FIs when deciding on the weightings, including when using automated risk assessment tools offered by external service providers.



International guidance documents (FATF, EBA) & **AMSF guidance & outreach** (e.g. Practical Guide for BRA + Part 1 of the Generic Guidelines + previous AML Tuesday presentations) give a range of information on the **risk factors, topics and types of data** to be considered for each risk category.

Such examples are **not exhaustive** – additional factors and information may need to be taken into account according to the variety of activities and complexity of the business.

B. Analysis of mitigation measures

- This phase relates to an assessment of the **level and adequacy of the risk mitigation measures** which are in place within the business.
- FIs must adopt **measures, policies, controls and procedures** that should prevent risks from materializing or mitigate their existence. The level of inherent ML/TF risk influence the type of controls and level of AML/CFT resources.
- Such controls should include **customer due diligence measures**, record-keeping & reporting measures, and measures relating to **risk management & internal controls**, such as client acceptance policies, procedures for customer risk assessment, compliance, independent testing of controls, standards for hiring and training employees, etc.
- The effects of such controls depend on their implementation in day-to-day operations. Therefore, their implementation should be **monitored on an ongoing basis**, to guarantee their effective application, determine their effectiveness and enable timely remediation of any gaps or issues.

Examples of information on controls to be considered

Since when has the control been implemented?	Dedicated resources to implement the control	Training provided to persons implementing the control	Level of oversight on the application of the control
Has the control been subject to independent testing?	Budget for EDD on (very) high-risk clients, e.g. obtaining external intelligence	Availability of reliable data on domestic & foreign BOs	Frequency of KYC reviews
Automatic versus manual controls	Periodic screening of whole customer database	Commercial databases used for sanctions & PEP screening	Responsibilities and timeframes for updating of sanctions lists

C. Residual risk response: Action plan

- Phase A & B should result in **the determination of the level of residual risk**: formed by the risks which remain after application of the controls.
- ML/TF/PF/C risk cannot be 100% eliminated regardless of how effective the control framework is.
- In this phase, the FI should verify whether the residual risks to which it is exposed are aligned with its **risk appetite:** the level of risk that it is willing to accept.
- The FI should put an **Action Plan** in place following the identification and assessment of inherent risk & controls.

D. Adoption

- The BRA and the Action Plan should be formalized in a **written document** (on paper or digital format).
- The document should be **approved by senior management** and be made **available to AMSF** upon request.
- It is also important that **employees are made aware of the results** of BRA, for instance through the ongoing employee ML/TF training programme. This ensures that employees are aware of the main risks that their entity is exposed to and that they can effectively execute the policies, procedures and controls determined by senior management to mitigate the risks.

E. Risk monitoring and review

- As ML/TF/PF/C risks evolve constantly, the BRA is a **cyclical process** that should be remain under regular review and updated on a periodic basis to ensure that **changing, new or emerging risks** are adequately taken into account.
- The BRA should be **updated periodically** on the basis of **(new) threats and vulnerabilities** that may be identified and take into account **any changes in the business model/clientele/activities** since the previous iteration.
- The BRA should be reviewed at least once a year. The exact scope/frequency of the updates should be **proportionate to the risks**. Reviews and updates should be **transparent and documented**.
- **Ad-hoc updates** are called for whenever there are **major developments** in management and operations (e.g. change in the business model, launch of a new product, implementation of new technologies, new geographic scope of business, change in clientele, risk exposure, etc.). FIs are recommended to develop an **internal list of trigger events** that trigger such ad hoc review.

03 Practical examples for FIs (per sub-sector)

Examples per sub-sector

Banking sector

Focus on assessing inherent risks relating to private banking

Asset management sector

Focus on assessing controls relating to PEPs

Life insurance sector

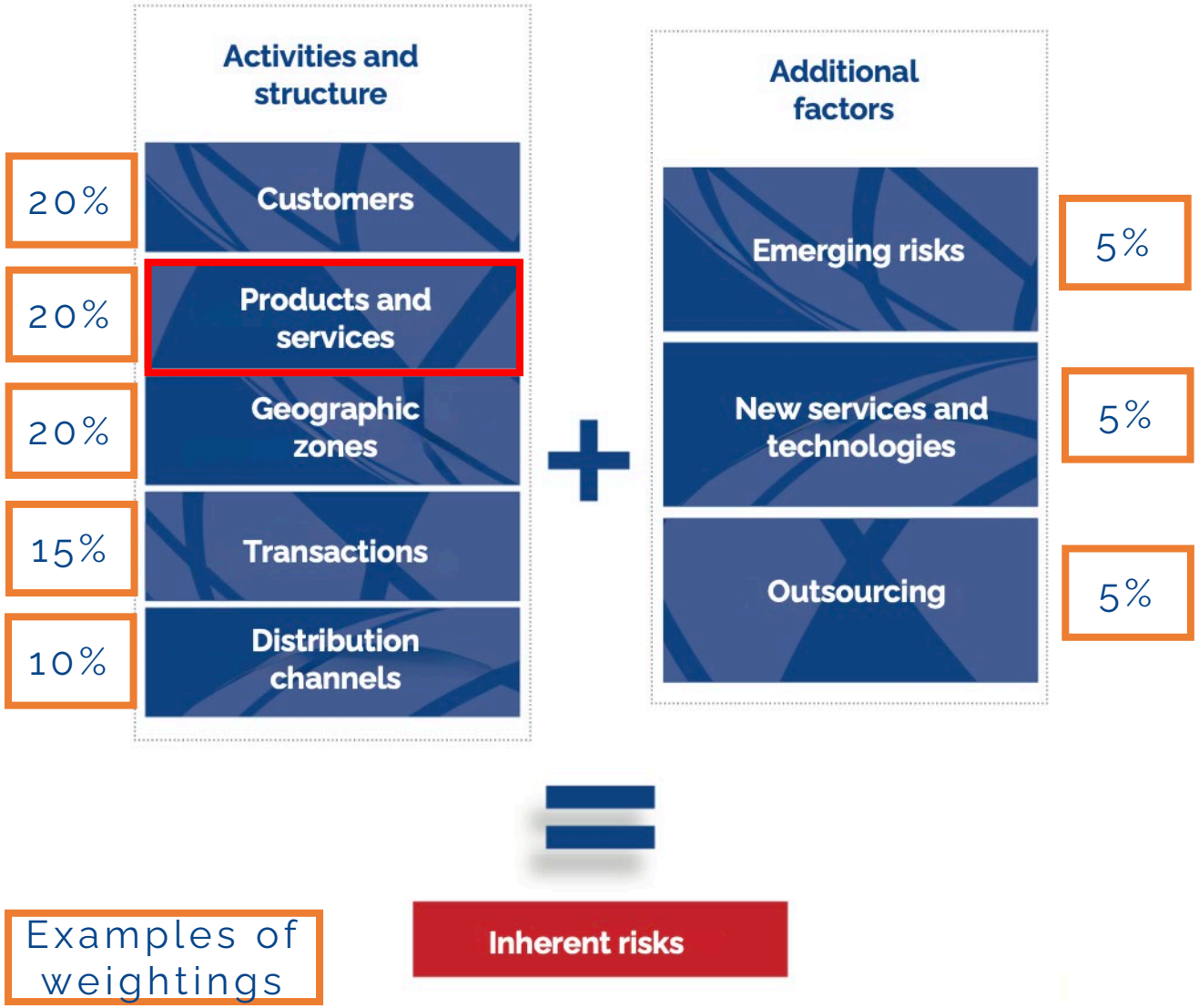
Focus on developing an Action Plan relating to sanctions screening

Private banking: High-level sources on risks

International guidance, typologies & evaluations	Information from professional sectorial bodies	Black lists, grey lists, sanctions lists
Topical risk assessments	**Monaco National Risk Assessment**	Sectorial risk assessments
(s)NRAs of other regions with links to the business	Communications by competent authorities	Guidance published by AMSF & Bar Association

- **FATF IN to R.10**, para. 15(c) lists private banking as high-risk service
- **EC's sNRA:** private banking is exposed to (very) significant ML threat & high inherent risks
- **Monaco NRA 2:** high risk rating for private banking sector
- **AMSF guidance** on private banking outlines examples of BRA risk factors for private banking

Private banking: Risk categories & risk factors



To measure inherent risk exposure, FIs need to chose a methodology, select a risk-rating scale and set parameters for risk ratings and weightings.

Illustrative example of such a methodology:

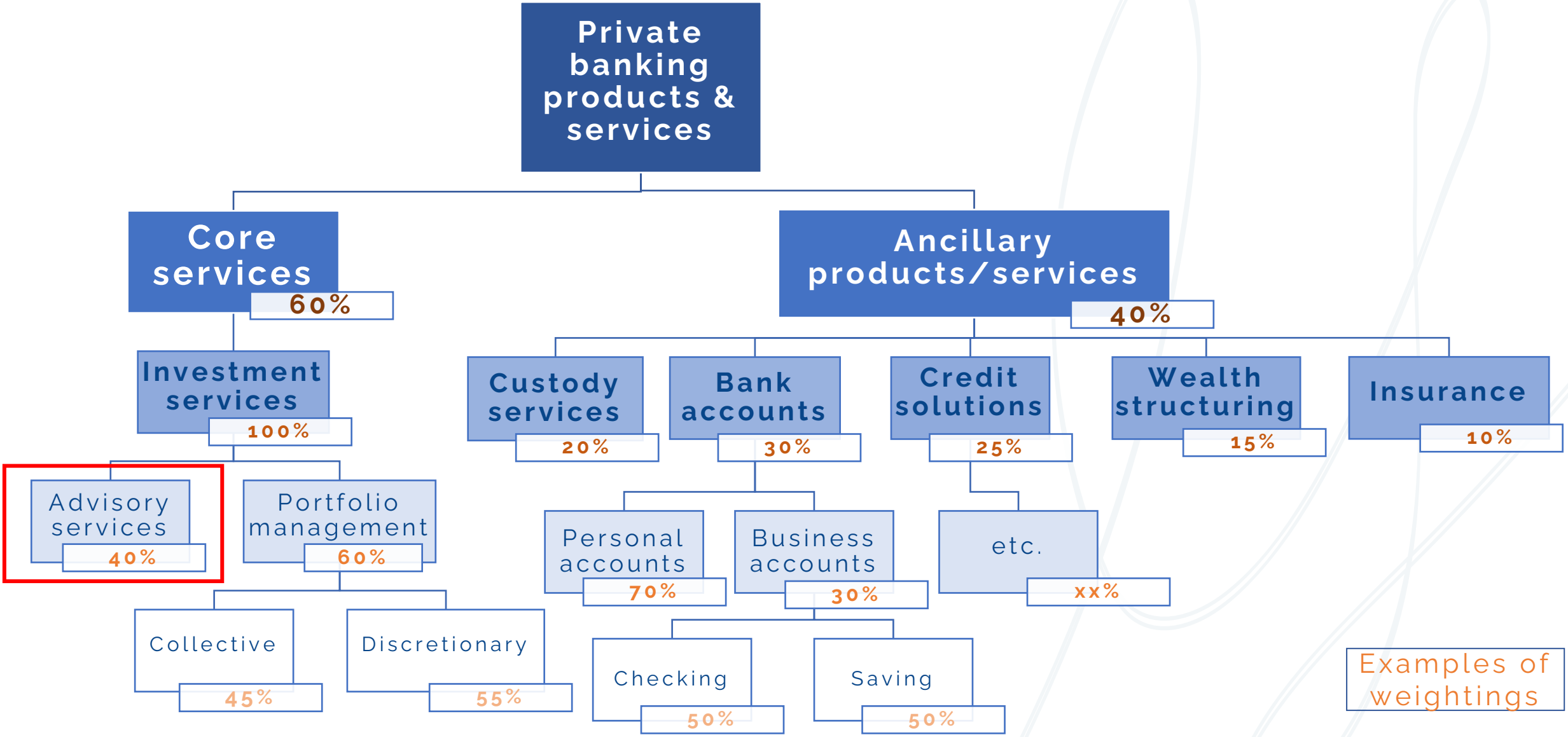
- Across all risk categories, an FI assesses a total of **50 risk factors.**
- Each of the 50 risk factors can receive a **risk rating** of **1 (very low risk) to 5 (very high risk).**
- Also, the relevance of each of the 50 risk factors receives a **weighting of 1 (limited relevance), 2 (relevant) & 3 (very relevant)** for the business.
- This results in **weighted risk ratings** for each risk factor on a scale of 1 to 15, e.g. a risk factor with a risk rating of 3 and weighting of 2 has a weighted risk rating of 6 (= 3 multiplied by 2).
- Under each risk category, an **average score of the weighted risk ratings** of the risk factors can be calculated
- The average scores of each risk category are then weighted according to the relative contribution of each risk category to the overall inherent risk, resulting in **an overall average risk score**, also on a scale of 1 to 15, with the parameters for final risk assessment set by the FI as follows: 1-5 Low risk; 6-10 Medium risk; 11-15 High risk.

Examples of **quantitative factors** to be taken into account when deciding on (sub-)weightings of inherent risk factors:

- Size of client base using each service
- Number of active products
- Volume of transactions under each service
- Contribution of each service to turn-over of bank

Examples of **qualitative factors** to be taken into account when assessing inherent risks associated to each service/product:

- Characteristics of the client base making use of the service/product
- Level of transparency or opacity offered by the service/product
- Level of complexity of the service/product, incl. geographic aspects
- Level/frequency/speed of transactions under each product/service, incl. any limits/caps and liquidity.


Private banking products & services
Core services
60%
Ancillary products/services
40%
Investment services
100%
Advisory services
40%
Portfolio management
60%
Collective
45%
Discretionary
55%
Custody services
20%
Bank accounts
30%
Credit solutions
25%
Wealth structuring
15%
Insurance
10%
Personal accounts
70%
Business accounts
30%
etc.
xx%
Checking
50%
Saving
50%
Examples of weightings

Simplified examples of risk factor analyses for investment advisory services

Risk category	**Products & services risk: Investment advisory services /** New services & technologies: Virtual assets	**Products & services risk: Investment advisory services /** Geographic risk	**Products & services risk: Investment advisory services**
Risk factor	Investment advice relating to virtual assets	Investment advice relating to remote markets	etc.
Description	Customers seeking advice / being advised on how to invest in virtual assets	Customers seeking advice / being advised on investments in products located in jurisdictions, possibly with weak AML/CFT regimes	etc.
Assessed risk level (1 to 5)	5 (Very high)	4 (High)	etc.
Weighting (1 to 3)	1 (Limited relevance)	3 (Very relevant)	etc.
Justification	It is very rare that customers seek investment advisory services on how to invest in virtual assets. It is not offered by the bankers on their own initiative..	It is relatively common for private banking customers to seek advice on investments in offshore jurisdictions, including jurisdictions with weak AML/CFT regimes – in 2023, approx. 10% of advisory services provided to customers related to investments in jurisdictions featuring on the FATF grey list, notably South Africa, Cayman Islands & UAE with fluctuations throughout the year due to regular changes of the list.	etc.
Weighted risk rating (1 to 15)	5 (Low risk)	12 (High risk)	etc.

Asset management sector: controls relating to PEP risks

- **Monaco NRA 2 (2021): not all asset management firms have a tool to detect PEPs,** which creates vulnerabilities for ML abuse.

- **Fictive example of Firm ABC:**
  - Firm ABC assessed its PEP controls in its 2022 BRA as **weak.**
  - ABC's senior management then endorsed the purchase and implementation of a **commercial tool that automates PEP screening**. The tool came into effect in the beginning of 2023.
  - Through the use of the new tool, ABC has identified **additional PEPs** in the existing client base which had not been previously detected and acknowledged in previous BRAs.
  - Also, throughout the past year, the firm **onboarded several new clients/clients with BOs** who qualify as PEPs, including some PEPs who are also HNWIs and some foreign PEPs.
  - The BRA update conducted early 2024 concluded that inherent PEP risks have increased (and are higher than previously assumed) and has analysed the **adequacy and strength of the newly enhanced PEP controls.**

Information on PEP controls to be considered

Since when has the control been implemented?	Dedicated resources to implement the control	Training provided to persons implementing control	Level of oversight on the application of the control
Has the control been subject to independent testing?	Budget for EDD for high-risk clients	Availability of reliable data on domestic & foreign BOs	Availability of reliable means for identification
Automatic versus manual controls	Periodic screening of whole customer database	Commercial databases used for sanctions & PEP screening	Responsibilities and timeframes for updating of sanctions lists

Factors contributing to risk mitigation score for PEPs

- Fictional examples of factors that contribute to increasing the risk mitigation score for PEP controls in Firm ABC:
  + Automated PEP screening system through commercial database has been implemented
  + New screening system has been used to screen all existing clients to detect additional PEPs
  + Remediation project ongoing to implement EDD for all detected PEPs and nearly completed
  + Opinion/advice of compliance officer is henceforth sought for every new PEP client and senior management gives final approval of all new PEP clients
  + KYC data for each PEP client is updated at least once a year
  + Client-facing staff have received specific training on onboarding and reviewing PEP customers
- Fictional examples of factors that contribute to moderating the risk mitigation score:
  - The new control (automated screening) has been implemented less than one year ago
  - Legacy issues: the remediation process to apply EDD to newly detected PEPs among existing clients has not been fully completed yet – for 20% of files, additional documentation, e.g. on SoW, is pending.
  - The new control has not been subject to independent testing yet – this is planned for later in 2024.

Risk category	Risk factor	Weighted risk rating (1 – 15)	Risk mitigation measures in place	Estimated impact of mitigation	Residual risk (1 – 15)
Customer risk	Customer, or BO of customer is a PEP, raising risks in particular in relation to laundering of proceeds of predicate offenses such as corruption, embezzlement and influence peddling	12 (High)	New automated screening system in place (<1 year) which improved detection rate. Oversight by compliance Senior management approval Enhanced monitoring, incl. more frequent KYC updates PEP training for frontline staff Pending legacy issues in relation to 20% of files for PEPs onboarded prior to new tool Independent test of new control planned for Q3-2024	30%	8,4 (Medium -High)

Life insurance sector: Fictional example of Action Plan

- A life insurance brokerage company has identified **some gaps in controls relating to sanction screening**, resulting in inadequate mitigation of customer risks, particularly **terrorist financing risks** (in relation to individuals/entities on terrorist sanction lists) as well as corruption risks and other risks of sanction evasions (e.g. in relation to Russian oligarchs/war facilitators). This results in a high level of risk that is not acceptable under the company's **risk appetite**.
- Also, this means that the company does not fully comply with **legal obligations for the timely and full implementation of sanctions applicable in Monaco, which apply regardless of the risks.**
- For the time being and given the relatively small size and low level of activity of the company, there is no budget for the purchase of an external automated tool that conducts automated sanctions screening. The company therefore outlines concrete steps in its BRA Action Plan for **the enhancement of the existing manual controls**.
- Once these steps are approved by senior management, the company will proceed to **update its procedures** to reflect the changes and to assign the related roles/responsibilities. Staff will be informed of the changes and receive **training** through a dedicated information session to be organised by the compliance officer.
- The adequacy and strength of the enhanced manual controls as well as the real additional costs they bring about in terms of resources will be assessed at the **next iteration of the BRA**. It can then be assessed to what extent they help to The Board will then consider whether to proceed with this solution or whether to invest in an automated tool.

Action plan to enhance sanction-related controls

Enhancements of controls compared to existing situation are highlighted in green.

- Extension of the relevant parties to be screened for sanctions:
  - Customers
  - BOs
  - Representatives of the customers
  - Directors of legal person customers
  - Beneficiaries of insurance policies
  - Any third parties involved in customer transactions
- More frequent and quicker screening of all of the above parties against sanctions lists:
  - Each time the National List is updated - the screening of all existing parties against new additions to the list is to be completed within 24 hours (as compared to 72 hours previously)
  - Before entering in a new business relationship
  - During periodic KYC reviews
  - When changes are made to existing information on customers, BOs, beneficiaries of insurance policies etc., within 24 hours (as compared to 72 hours previously)
  - Before processing any type of transaction

Some final points of attention

- When FIs use automated IT systems to decide and allocate risk ratings, weightings and overall risk scores and do not develop these inhouse but rather purchase them from an **external provider,** they should ensure that:
  - They **participate** in the development of the risk rating methodology and drafting of the document
  - They **fully understand** the risk rating methodology proposed by the external provider and how it combines risk factors to achieve an overall risk score;
  - They ensure that the BRA is **adapted** to their own activities
  - They can satisfy themselves that the scores allocated are **accurate** and reflect the entity's **understanding** of ML/TF risk.
  - They should be able to **demonstrate** this to the competent authority.
- A generic ML/TF risk assessment that has not been adapted to the specific needs and business model of the firm ('an **off-the-shelf ML/TF risk assessment**') will not meet the legal requirements and AMSF's expectations.
- **Firms which are part of a group** should also proceed to conduct an individual assessment and cannot solely rely on the global risk assessment of the group.

FINANCIAL TRANSPARENCY ADVISORS

Thank you for your time

Financial Transparency Advisors GmbH
Zieglergasse 38/7/1070 Vienna, Austria

Phone: +43 1 890 8717 11

www.ft-advisors.com

http://www.ft-advisors.com

Next Session:

21.05.2024

Topic:

Customer Risk Assessment

Today's Host: Tamar Goderdzishvili

Today's Presenter: Suzanna van Es