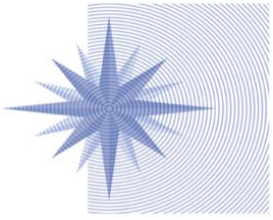

Banco Santander
Bank of America
Barclays
Citigroup
Deutsche Bank
Goldman Sachs
HSBC
JPMorgan Chase
MUFG Bank
Société Générale
Standard Chartered Bank
UBS

the Wolfsberg Group

Guidance on the Risk-Based Approach

The application of a risk-based approach (RBA) is critical to the effective design and maintenance of a financial institution's (FI's) financial crime risk management (FCRM) programme,[1] covering its risk appetite, policies, measures and controls.

The Wolfsberg Group (the Group) first recognised the importance of an RBA in 2006, when it published the original version of this paper, *Guidance on an RBA for Managing Money Laundering Risks,* and the topic has continued to be widely discussed across the private and public sectors. In light of the current standard setting and regulatory reform agenda, and the Group's collaboration with the Financial Action Task Force (FATF) on the RBA, the Group has taken the opportunity to define the core elements of an RBA through our *Statement on the RBA*[2] and by updating this guidance.

Aligned with the FATF, the Group considers an RBA to mean that countries, competent authorities and FIs should be expected to identify, understand and assess the financial crime risks to which they are exposed, and take proportionate action that "appropriately corresponds to the level of identified risk and effectively mitigates the risks."[3] An RBA underpins effective financial crime risk management by enabling FIs to focus on responding to their highest priority threats while stopping, reducing and/or redesigning activities that do not contribute materially to the fight against financial crime. In today's dynamic financial crime risk environment, and given unprecedented levels of innovation and technological advancement, the need for an RBA has never been greater. Leadership, whether in the public or the private sector, should reinforce this through a strong "tone-from-the-top" that establishes a clear risk-based commitment to effective financial crime risk management.

As outlined in the *Statement on the RBA,* the Group recommends that FIs should demonstrate three key elements when designing and maintaining a risk-based FCRM programme: **proportionality**, **prioritisation** and **effectiveness**. This guidance will elaborate on these elements by detailing strategies and mechanisms that FIs could adopt when implementing an RBA. As the RBA is integral to several areas of focus for the Group, this guidance should be considered alongside other Group resources, which have been referred to where appropriate.

[1] In this Guidance, the Group refers to "financial crime" risk management given most FI FCRM programmes cover more than anti-money laundering (AML). References to AML are also inclusive of counter-terrorist financing and counter-proliferation financing, in line with industry practice.
[2] The Wolfsberg Group - Statement on the Risk-Based Approach
[3] FATF Recommendations, Rec 1 INR glossary (2025)

Proportionality: an FI should design and maintain a FCRM programme proportionate to its business model as determined by its size, scale, footprint, customers and risk appetite (as informed by its assessment of risk).

Each FI is distinct, and a one-size-fits-all approach to financial crime risk management is not a risk-based approach. Each FI should have a FCRM programme that is proportionate to the level of financial crime risk inherent in its business strategy and operating model, and a variety of mechanisms can be used to identify, assess and manage those risks.

National risk assessments, priorities and strategies (where available) identify a country's financial crime risks, threats and vulnerabilities, and outline public authorities' focus areas. FIs can leverage insights from such assessments to inform and prioritise risk-based FCRM programme design, while also applying the concept of proportionality by focusing on the elements that apply specifically to them, based on their business model. Open and constructive **dialogue with the public sector, including law enforcement,** can also yield valuable insights on emerging threats and risks. As outlined in the Group's work on *Effectiveness through Collaboration,*[4] collaboration and dialogue will lead to far better outcomes than initiatives pursued in a silo, enabling FIs to fulfil their obligations, assist national authorities in combating financial crime more effectively and reduce the risk of divergence in the application of an RBA.

Establishing a **financial crime risk appetite** can determine the strategic and proportionate boundaries of an FI's FCRM programme. Set by senior management, risk appetite should define the level of financial crime risk an FI will accept to meet its objectives, the risks it will not tolerate, and considers the FI's values, regulatory obligations, business goals and risk management framework. FIs must also take financial inclusion expectations into account when defining their financial crime risk appetite, while ensuring not to compromise on robust financial crime risk management.[5]

Business wide risk assessments use risk-focused data across categories such as customers, transactions, geographies, products and delivery channels, to assess quantitatively and qualitatively the holistic risks to which an FI is exposed and can be used to inform an RBA. Targeted risk assessments, such as those focused on **customer, industry, country**[6] and **product**, can also be used to segment inherent financial crime risk (commonly using ratings of low, medium and high) and guide risk-based measures and controls, including, for example, the level of customer due diligence (CDD), approval requirements, frequency of review, necessary governance and escalation protocols and ongoing monitoring for suspicious activity. However, the assessment of financial crime risk should also be a **dynamic process** embedded within business-as-usual (BAU) risk management activities, including, for example, through regular oversight and reporting on management information and control effectiveness, providing FIs with valuable insights for use on an ongoing basis to maintain a proportionate and relevant RBA.

FIs should **avoid ineffective practices** when designing and implementing an RBA. Risk assessments should be aligned and mutually reinforcing, as duplication, inconsistency or siloed approaches undermine the integrity of a FCRM programme. Innovation and technology should also be leveraged

[4] The Wolfsberg Group – Effectiveness through collaboration

[5] FATF's amendments to R.1 and updated Guidance on Financial Inclusion prompt countries to promote financial inclusion by increasing focus on proportionality and simplified measures under the RBA. As stated in the Group's response to FATF's public consultation on AML/CFT and financial inclusion, FIs servicing customers who would otherwise be excluded from the financial system should undertake "alternative measures" focused on addressing the unique risks represented by the customer in a distinct manner.

[6] The Wolfsberg Group – Country Risk FAQs

to deliver scalable, effective risk management, faster responses to business and regulatory demands, greater proactivity and improved operational efficiency.

Prioritisation: an FI should prioritise attention, and the allocation of resources, to higher risk customers and activities, which may also entail stopping, reducing, and/or redesigning existing measures that are determined to be redundant, duplicative or unproductive from a risk management perspective.

A focus on everything is a focus on nothing. Prioritisation helps FIs respond dynamically to an ever-changing risk landscape by directing attention and resources towards higher-risk customers and activities, while reducing effort where risk is lower. By understanding the risk variables linked to who the customer is and what the customer does, FIs can identify the highest-risk areas to prioritise and mitigate. Risk variables include, but are not limited to:

Who the customer is

- **Customer types:** FIs should take steps to identify the characteristics of customer types that may potentially present higher inherent financial crime risk, for example, non-resident customers, companies with nominee shareholders or shares in bearer form.
- **Industry/business types:** FIs should determine the characteristics of customers operating in potentially higher risk industries or businesses, for example cash intensive retail and personal-service businesses, money service businesses, and third-party payment processors.
- **Customer structure (legal entity):** understanding a customer's ownership structure and the rationale for it is key to identifying financial crime risk. Simple structures offer transparency. Complex structures require assessment of whether the complexity is commercially justified and consistent with the customer type, sector and products/services, or whether it may be intended to obscure illicit activity. Also consider the entity's formation date, as newly established entities may pose higher risk than those that are well-established.
- **Publicly owned and traded customers (legal entity):** companies and their wholly owned subsidiaries that are publicly owned or traded on a recognised exchange generally present reduced financial crime risk, as they are typically subject to multiple disclosure obligations in line with the requirements of their home country regulations. Such corporates may present FIs with an opportunity to decrease the intensity and frequency of FCRM measures and controls.
- **Customers resident, incorporated, or conducting significant business in higher risk countries:** when prioritising measures and controls, consider credible assessments of weaknesses in a country's FCRM regime, for example, FATF listed jurisdictions, and whether a customer's exposure to those countries is a relevant risk factor requiring consideration.

What the customer does

To understand customer behaviour, FIs should focus on how a customer uses products and services, moves value, and interacts with the FI over time. Behavioural risk indicators are context-dependent and should be assessed against the customer's stated financial needs, purpose of the account, expected activity and known profile. Risk variables include, but are not limited to:

- **Customer profile:** longstanding relationships may provide a better view of customer behaviour and risk profile. Over time, refreshed CDD, transaction history and regular contact can improve the FI's understanding of the customer's risk. However, repeated and/or unusual amendments to key customer profile information, particularly where there is no clear business rationale, may be an indicator of risk, including evasive or obstructive conduct, unexplained delays in

responding to customer outreach, incomplete responses or documentation that is inconsistent or contradictory.

- **Transactional behaviour:** unusual transactional behaviour, particularly where it does not align with the customer's stated purpose of account, expected turnover, wealth, size and volume of transactions or business model, may be an indicator of risk. Consideration may also be given to activity involving higher-risk corridors or jurisdictions that do not align with the customer's known profile or the markets they expect to transact with.
- **Product usage:** unusual use of products, particularly where there is no clear business rationale, may be an indicator of risk. This may include attempts to misuse product features or access methods in a manner that may increase anonymity, add complexity and/or reduce end-to-end traceability.
- **Customer risk insights:** various financial crime control elements, such as screening and monitoring for suspicious activity,[7] enable FIs to identify risks associated with customer attributes, behaviour and transactions. Customer risk insights should also be used to determine the higher-risk areas to prioritise and mitigate as part of an RBA.

FIs must, however, apply sound judgement when assessing risk variables, including evaluating whether customers align with the organisation's risk appetite, and tailoring controls and measures to reflect the risks associated with different customer profiles.

Effectiveness: an FI should focus on effective outcomes, as aligned to the Group's work on *Demonstrating Effectiveness*[8], facilitating a more responsive, forward-looking and dynamic approach to risk management, rather than applying a one-size-fits-all, rules-based only approach.

Effectiveness is an integral part of an RBA and has been central to the Group's work for several years. An FI can demonstrate an effective and risk-based approach to identifying, assessing and managing its risks by adopting, at its core, the elements that the Group has identified as key components of effectiveness. The Wolfsberg Factors as outlined in the Group's *Statement on Effectiveness,*[9] set out three key elements of an effective FCRM programme:

1. Complying with AML/CTF laws and regulations.
2. Establishing a reasonable and risk-based set of controls to mitigate the risks of an FI being used to facilitate illicit activity.
3. Providing highly useful information to relevant government agencies in defined priority areas.

Building on the Wolfsberg Factors, the Group's paper on *Demonstrating Effectiveness*[10] provides further guidance on how an FI could assess risk in defined priority areas and demonstrate the effectiveness of its FCRM programme by evolving to focus more on effective outcomes. Further, the Group's paper on *Auditing for Effectiveness*[11] outlines the key principles and measures that internal audit should apply when measuring the effectiveness of a FCRM programme. This includes demonstrating appropriate governance, adherence to all relevant local laws and regulations, design

[7] The Wolfsberg Group Statement on Effective Monitoring for Suspicious Activity Part I and Part II.

[8] The Wolfsberg Group – Demonstrating Effectiveness

[9] The Wolfsberg Group – Statement on Effectiveness

[10] The Wolfsberg Group – Demonstrating Effectiveness

[11] Wolfsberg Group Principles for Auditing for Effectiveness

and operating effectiveness of controls and the establishment of mechanisms that allows for the sharing of highly useful information with relevant government agencies.

An effective RBA should also be underpinned by traceable governance mechanisms that ensure transparency in decision-making, processes and controls, in order to maintain trust with supervisors and auditors. FIs should, however, aim to ensure that governance remains effective, avoiding unnecessary complexity that can impede decision-making and divert resources from core risk management activities.

Risk-based supervision

FIs need flexibility to implement and evidence an RBA. A supervisory and examination regime across supervisors and internal/external auditors, which supports an RBA – including moving away from lower-value measures and controls – is critical to success in the fight against financial crime. Supervisors and auditors should "move beyond a tick-box approach in monitoring the private sector's efforts"[12] and not focus on the mere existence of information or setting unrealistic expectations (such as a "zero-failure" compliance environment or "no SAR left behind"[13]). These can divert resources from effective risk management, increase costs and create unnecessary customer friction without improving (and often worsening) financial crime risk management outcomes.

Supervisors and internal/external auditors should prioritise assessing FCRM outcomes and the practical contribution made in the fight against financial crime. Testing standards should be tailored to each FI's business model and risk profile, avoiding a one-size-fits-all, rules-based only approach, so FIs can evidence effectiveness through proportionate and prioritised RBA design and implementation. Ongoing public-private collaboration, consultation and regular auditor dialogue will be key to the acceptance of an RBA that aligns to each FI's unique risks and business profile.

Training and Culture

People are critical to maintaining an FI's systems and controls to prevent and detect financial crime, and "applying a risk-based approach to the various methods available for training, gives each financial institution additional flexibility regarding the frequency, delivery mechanisms and focus of such training."[14] Staff in higher-risk roles should receive targeted, role-specific training and hone the skills required to identify, assess and manage financial crime risks effectively. Learning should also keep pace with technological change and innovation, so staff understand new tools and processes and can use them confidently to improve financial crime risk management outcomes.

Learning programmes should build out capabilities in critical thinking and fostering curiosity so employees can apply appropriate judgement, spot risks and make informed decisions. Training should also encourage staff confidence to speak up and escalate concerns, supporting a proactive risk-based culture. Leadership should set a strong 'tone-from-the-top' by promoting the importance of financial crime risk management, leading by example and prioritising continuous learning, ensuring decision-making is genuinely risk-based and FCRM programmes deliver effective outcomes.

[12] FATF Guidance on Risk-Based Supervision
[13] For more information on the "no SAR left behind" concept, which refers to ensuring that no historical SAR/STR is "left behind" when transitioning to new monitoring approaches (and often results in ineffective and over-alerting monitoring programmes), see our statements on monitoring for suspicious activity: The Wolfsberg Group Statement on Effective Monitoring for Suspicious Activity Part I and Part II.
[14] FATF Guidance on Risk Based Approach – High Level Principles and Procedures

Conclusion

Applying an RBA is essential to an FI's FCRM programme. It ensures resources are focused on the highest-priority risks and threats, while stopping, reducing and/or redesigning activities that do not materially strengthen the fight against financial crime. By drawing on the Group's key components of **proportionality, prioritisation** and **effectiveness**, and utilising this guidance, FIs can demonstrate a credible approach to the design and implementation of an RBA that is right for their organisation. This will only be possible with a supervisory and examination regime that enables, rather than hinders, an RBA, giving FIs the flexibility to implement and evidence an approach tailored to their risk profile, moving beyond tick-box compliance and focusing on outcomes that demonstrably improve risk management effectiveness. When applied well, an RBA strengthens outcomes for both the private and public sectors and reinforces our shared responsibility to prevent, detect and disrupt financial crime where it matters most. The Group will continue to collaborate with the FATF, and more broadly across the industry, to advance the shared priority of embedding a genuine RBA.