هيئة الأوراق المالية والسلع
SECURITIES & COMMODITIES AUTHORITY

United Arab Emirates

Obligations to implement Business Wide Risk Assessment

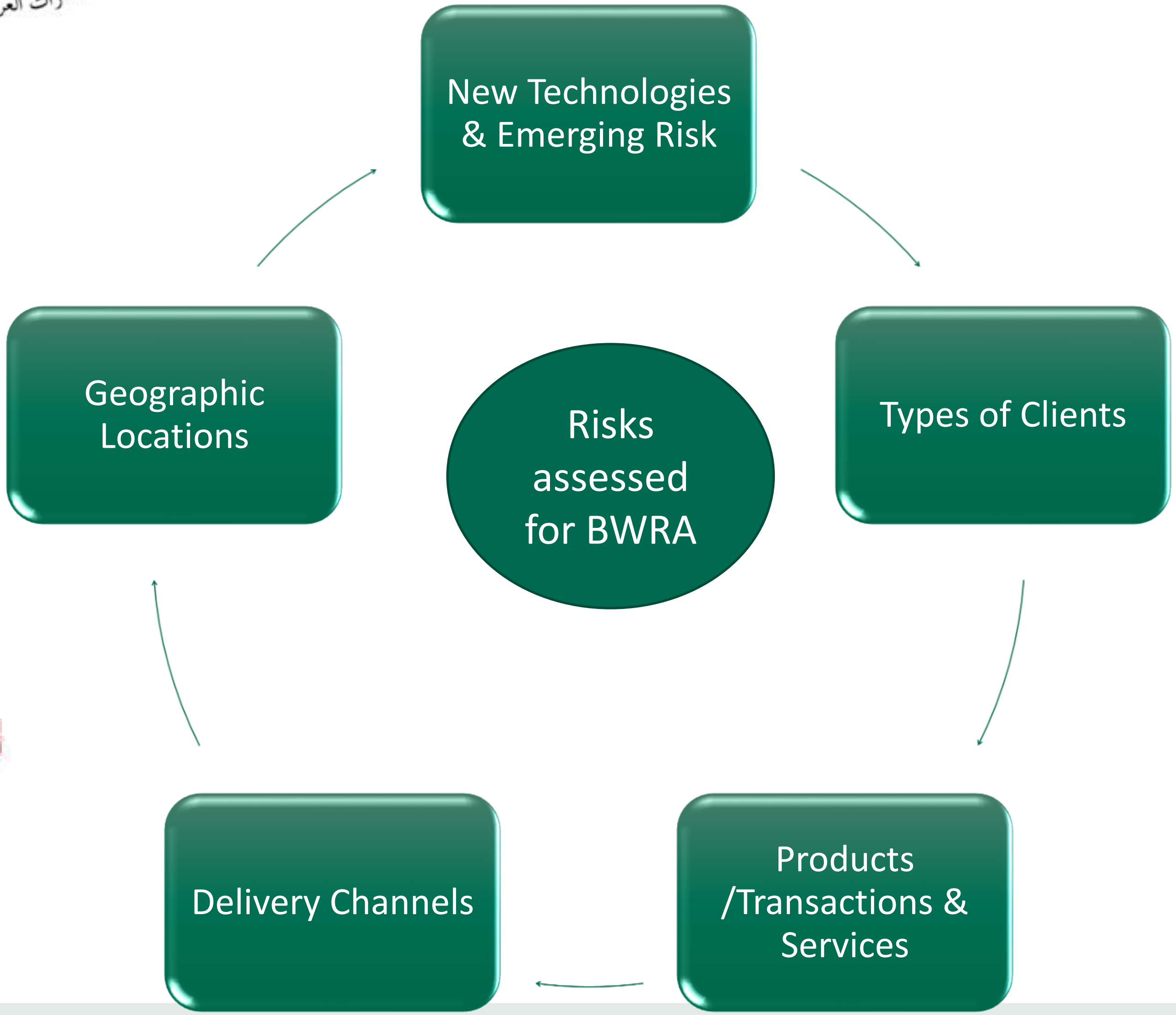
Federal Authority | هيئة اتحادية

Defining Business Wide Risk Assessment

BWRA is a fundamental step for an effective implementation of AML and CFT compliance framework.

It is considered a strategic business discipline that enables Financial Institutions to achieve their objectives by **identifying**, **understanding** and **assessing** the full spectrum of AML/CFT – Targeted Financial Sanctions (TFS), and Proliferation Financing (PF) risks.

Key Risk Categories in BWRA




Financial
Hazards
Operational
Reputation
Strategic
Business

Phases of BWRA

Building an Effective BWRA Program

Phase 1 : planning and scoping	Phase 2: Implementation			Phase 3: Results & recommendation
Scope	**Assess Inherent risk**	**Implement Controls**	**Define Residual Risks**	**Action Plan and reporting**
Define the scope and structure of business areas in order to assess the business units, divisions, branches, countries and regions	Select risk areas and factors to assess inherent risk based on empirical data analysis and analytical techniques for both ML/FT risks	Design and implement controls to ensure mitigate any risk.	Evaluate results and set the institution's risk appetite statement-	Develop action plan for underperforming controls based on identified gaps, create reporting, and prepare documentation for audit / exam purposes

Phase 1: Scope

Business Units:

- Assess each unit within the organization, considering its specific functions, processes, and risk exposure.
- Include front-line units, back-office operations, and support functions.

Legal Entities:

- Evaluate all legal entities under the corporate umbrella, including subsidiaries, joint ventures, & partnerships.
- Consider the legal and regulatory environments of each entity.

Divisions:

- Break down larger business segments into divisions for a more detailed assessment.
- Focus on the unique risks and controls relevant to each division.

Countries and Regions:

- Analyze risks based on geographic location, considering local laws, economic conditions, and political stability.
- Differentiate between domestic and international operations.

Phases of BWRA

Building an Effective BWRA Program

Phase 1 : planning and scoping	Phase 2: Implementation			Phase 3: Results & recommendation
Scope	**Assess Inherent risk**	**Implement Controls**	**Define Residual Risks**	**Action Plan and reporting**
Define the scope and structure of business areas in order to assess the business units, divisions, branches, countries and regions	Select risk areas and factors to assess inherent risk based on empirical data analysis and analytical techniques for both ML/FT risks	Design and implement controls to ensure mitigate any risk.	Evaluate results and set the institution's risk appetite statement-	Develop action plan for underperforming controls based on identified gaps, create reporting, and prepare documentation for audit / exam purposes

Phase 2: Inherent risk Assessment

Risk Identification: The first step involves identifying the various risks of ML/TF that the enterprise might face. This includes understanding the types of **customers**, the nature of the **products** or **services** offered, the **channels** through which **transactions** occur, and the **geographic** locations involved in the business operations.

Risk Analysis: Once risks are identified, the next step is to assess their **severity** and **likelihood** of **occurrence**. This involves evaluating how vulnerable the FI's products, services, and operations are to ML/TF activities and the **potential impact** if such activities were to occur.

Example: Inherent Risk Analysis *(For illustrative Purposes)*

Severe	Potential criminal prosecution against the firm
Significant	Major supervisory action against the firm and significant reputation damage to the firm
Moderate	Supervisory action against the firm and some reputation damage to the firm
Minor	Negligible reputation damage to the firm

Very likely	There is a very high chance of ML/TF occurring in this area of your business
Likely	There is a moderate chance of ML/TF occurring in this area of your business
Possible	There is a small chance of ML/TF occurring in this area of your business
Very unlikely	There is a very little chance of ML/TF occurring in this area of your business

Likelihood scale	Very likely				
	Likely				
	Possible				
	Very unlikely				
		Minor	Moderate	Significant	Severe
	Impact scale				
Risk rating		Low	Medium	Medium-High	High

Example: Inherent Risk Identification/Classification *(For illustrative Purposes)*

	Low	Medium	High
Client base	o Small local businesses, o Low net-worth individuals/ Clear source of wealth o Fixed ownership and business model, o Simple corporate structure, o Well-known client base o Small number high-risk clients	o Mostly local, o Fixed ownership and nature of business of international clients o Simple corporate structure o Moderate number high-risk clients	o High percentage of international clients, o Low transparency of Beneficial Owners o Trust clients o Convicted clients o Clients with cash intensive business o Clients dealing in cryptocurrencies o Complex Group Structures o Complicated process of establishing SoF/SoW o PEPs o High-risk AML/CFT jurisdictions o High-risk jurisdictions subject to UN/EU Sanctions, embargoes, bans o Large number of high-risk clients

(1) : Individual Customer Risk Scoring

- Individual Customer Risk Scoring, based on Factors as:
  - Customer type (e.g., PEPs, non-residents, high-net-worth)
  - Business relationship complexity
  - Use of intermediaries
  - Links to high-risk sectors or jurisdictions
  - Source of funds,
  - Geographic location,
  - Products or Services
  - Historical transaction behavior.

(2) : Segmentation

- Segment the clients into categories, such as:
  - Local Customers
  - International Customers
  - PEPs
  - Small Local Companies
  - Large Complex Structured Companies
  - Give a Weighted Average for each category

(3) : Aggregated Risk Analysis

- After the Segmentation process, the FI should assess the Impact and Likelihood for each category, through:
- Qualitative Assessment
- Quantitative Assessment

(4) : Weighted Overall Risk

- Considering the proportion of each customer category relative to the total customer base.
- Applying a weighting to each category based on its size.

For example, if the proportion of high-risk customers is significant, the institution's overall risk level increases.

- Evaluating the potential impact on the institution (financial, legal, and particularly in relation to financial crime risks).

Example: If the proportion of high-risk customers such as PEPs is very low (e.g., 5%), the institution may assess the overall risk as moderate after applying controls.

However, if this percentage is high (e.g., 30%), the institution may classify the risk as very high and implement more stringent risk mitigation measures.

Phases of BWRA

Building an Effective BWRA Program

Phase 1 : planning and scoping	Phase 2: Implementation			Phase 3: Results & recommendation
Scope	**Assess Inherent risk**	**Implement Controls**	**Define Residual Risks**	**Action Plan and reporting**
Define the scope and structure of business areas in order to assess the business units, divisions, branches, countries and regions	Select risk areas and factors to assess inherent risk based on empirical data analysis and analytical techniques for both ML/FT risks	Design and implement controls to ensure mitigate any risk.	Evaluate results and set the institution’s risk appetite statement-	Develop action plan for underperforming controls based on identified gaps, create reporting, and prepare documentation for audit / exam purposes

Phase 2: Set Controls

❖ Control Categories:

(For illustrative Purposes)

- Corporate Governance, Management Oversight and Accountability
- Policies and Procedures
- (SDD), (CDD), (EDD), and (PEPs)
- Historical Risk Assessments
- Management Information System (MIS) / Reporting
- Record Keeping and Retention
- Designated AML/CFT Officer
- SAR/STR Filing
- Ongoing Monitoring and Controls
- Training Programs
- Independent Testing and Audit
- Other Controls

91-100% — **Satisfactory:** Substantially meeting all control requirements

75-90% — **Needs Improvement:** Meeting between 75% and 90% of control requirements

<75% — **Unsatisfactory:** Meeting less than 75% control requirements

Phase 2: Set Controls- *(For illustrative Purposes)*

1.Identification of Key Controls:

- Determine the controls used to mitigate inherent ML/TF risks.

Classify controls as:

- **Preventive** (e.g., CDD/EDD procedures),
- **Detective** (e.g., transaction monitoring systems),
- **Corrective** (e.g., client exit procedures).

2.Development of Control Questionnaires:

- Create detailed questionnaires for each control type.

Evaluate:

- Design appropriateness,
- Implementation consistency,
- Operational effectiveness.

3.Control Self-Assessment:

- Conduct internal evaluations using the questionnaires.
- Evidence-based responses,
- Identification of control gaps or weaknesses.

4. Involvement of SMEs:

- Engage independent experts to review and challenge assessments.
- Ensure comprehensive analysis and avoid internal bias.
- SMEs provide benchmarking insights and best practices.

5. Independent Audit & Compliance Testing:

- Leverage findings from, Internal audit functions, External audits and Regulatory inspections.
- Compare audit results with self-assessment outcomes for a holistic view of control strength and residual risk

6. Continuous Improvement

Use the insights gained to:

- Enhance control frameworks,
- Prioritize remediation,
- Strengthen risk governance.

Phase 2: Derive the Residual Risk-

- Residual risk is determined by balancing the inherent risk with the overall strength of the risk management activities/controls
- The residual risk rating is used to assess whether the ML/FT risks within the business unit as well as for the institution as a whole are being adequately managed
- The residual risks should be calculated across each business unit
- The residual risks should be available in a visual heatmap format

(For illustrative Purposes)

Residual Risk Determination		Inherent Risk		
		Low	Medium	High
Control Assessment	91 – 100% Satisfactory	Low	Low	Medium
	75 – 90% Needs Improvement	Low	Medium	High
	<75% Unsatisfactory	Medium	High	High

Phases of BWRA

Building an Effective BWRA Program

Phase 1 : planning and scoping	Phase 2: Implementation			Phase 3: Results & recommendation
Scope	**Assess Inherent risk**	**Implement Controls**	**Define Residual Risks**	**Action Plan and reporting**
Define the scope and structure of business areas in order to assess the business units, divisions, branches, countries and regions	Select risk areas and factors to assess inherent risk based on empirical data analysis and analytical techniques for both ML/FT risks	Design and implement controls to ensure mitigate any risk.	Evaluate results and set the institution's risk appetite statement-	Develop action plan for underperforming controls based on identified gaps, create reporting, and prepare documentation for audit / exam purposes

Phase 3: Reporting and updating

1. Annual Review of ML/TF and Sanctions Risk

- Conduct the BWRA at least once annually, or if:
  - Significant changes occur in the institution's risk profile.
  - New threats or regulatory guidance emerge.
  - Internal audits or inspections identify major gaps.

2. Trigger-Based Updates, in instances:

- Launching new products, services, or delivery channels.
- Expansion into new geographic locations or customer segments.
- Regulatory or legal changes impacting AML/CFT obligations.

- **3. Communication and Governance**
- **Timely communication** of BWRA findings to:
  - **Board of Directors** – to ensure strategic oversight.
  - **Risk and Compliance Committees** – for governance and mitigation decisions.
  - **Senior Management** – to implement controls and resource allocation.
- Ensure decision-makers are **fully informed** of identified risks, control effectiveness, and residual risks.
- **4. Documentation and Regulatory Expectation**
- Maintain comprehensive records of:
  - Risk assessment process and methodology.
  - Review frequency and decision rationale.
  - Approval by senior stakeholders.
- Be prepared to **demonstrate effectiveness** to regulators.

Controls Gap Analysis

1. Control Gap Analysis

- When additional AML/CFT or sanctions-related controls are needed to manage **residual risks**, the financial institution must:
  - Conduct a **control gap analysis**.
  - Compare existing controls to the level of controls required for effective risk mitigation.
  - Identify **gaps or deficiencies** in the current control environment.

2. Corrective Action Plans

- Action plans to address control weaknesses must be:
  - **Documented**, **measurable**, and **trackable**. Clearly defined with **implementation timelines**.
  - Structured to enable internal and external **auditors to validate** the adequacy and effectiveness of remediation steps.

3. Governance and Accountability

- Assign clear responsibility for each identified issue.
- Ensure that corrective measures are:
  - **Sustainable and permanent**,
  - Integrated into the institution’s long-term control framework..

هيئـة الأوراق الماليـة والسلـع
SECURITIES & COMMODITIES AUTHORITY
الإمارات العربية المتحدة

Phases of BWRA

United Arab Emirates

Building an Effective BWRA Program

Phase 1 : planning and scoping	Phase 2: Implementation			Phase 3: Results & recommendation
Scope	**Assess Inherent risk**	**Implement Controls**	**Define Residual Risks**	**Action Plan and reporting**
Define the scope and structure of business areas in order to assess the business units, divisions, branches, countries and regions	Select risk areas and factors to assess inherent risk based on empirical data analysis and analytical techniques for both ML/FT risks	Design and implement controls to ensure mitigate any risk.	Evaluate results and set the institution's risk appetite statement-	Develop action plan for underperforming controls based on identified gaps, create reporting, and prepare documentation for audit / exam purposes

BWRA Methodology – Expectation

- **Stand-alone Documentation Requirement:**
  - Maintain a detailed document explaining the methodology
  - Outline the processes, criteria and tools used
- **Methodology Explanation:**
  - Explain the methodology for identifying and evaluating risks, including the assessment of severity & likelihood.
  - Explain how vulnerabilities in products, services, & operations are analyzed.
- **Risk Identification Process:**
  - Detailed description of the process for identifying potential ML/TF risks, including customer types, geographic exposure, and products/services.
- **Use of Quantitative Analysis**
  - Include measurable data such as % of clients who are PEPs, number of high-risk customers on-boarded during the year, volume/ value of transactions to high-risk countries, % of assets in high-risk products, etc.
- **Severity and Likelihood Assessment:**
  - Clearly define criteria and scoring scales used to assess: Severity (impact of the risk event),Likelihood (probability of occurrence).
  - Use consistent scales (e.g., low, medium, high).
- **Vulnerability Analysis:**
  - Analyze internal gaps or weaknesses that may increase the risk to financial crime risk
  - Consider the effectiveness of internal controls, staffing, technology, and policy implementation
- **Impact Assessment:**
  - Assess potential financial, legal, regulatory and reputational impact.
  - Tailor assessments to the FI's size, complexity and client base.
- **Analysis of future outlook**
  - Include a future outlook section to anticipate emerging risks (e.g., fintech, digital assets, geopolitical instability).
  - Highlight plans for enhancements or adaptations to risk mitigation strategies.

هيئة الأوراق المالية والسلع
SECURITIES & COMMODITIES AUTHORITY

Key Record-Keeping for BWRA

1. Assessment Process Records:

- Model, methodology, procedures, findings.
- Organizational roles, process flows, timing, reporting, review/update requirements.

2. Risk Factor Documentation:

- Log all identified risks, inputs from internal sources (chief compliance officer, risk committee.. Or External Sources (NRA, FATF..)

3. Risk Mitigation Effectiveness:

- Adequacy and effectiveness of ML/TF and Sanctions Compliance controls.

4. Risk Analysis Records:

- Inherent and residual risk-factor analysis details.

5. Risk Level Determination:

- Final Overall risk, Threshold for acceptable risk levels, additional mitigating measures.

6. Policies & Procedures:

- Policies like customer acceptance, etc.

7. Risk Appetite Statement:

- Keep a formally documented risk appetite, reviewed and approved by senior management.

8. Information Sharing:

- Mechanisms for reporting to SCA and examiners.

9. Adjustment Evaluation:

- Improvements to risk mitigation procedures.

10.Corrective Action Plans:

- Detailed remediation plans, -
- Timelines, responsible parties, and status updates
- Methods for follow-up and audit validation.

Good and Bad Practices

Ineffective Risk Assessments: Generic and misaligned with company activities, systems, and customer profiles.

Lack of Integrated Frameworks: No flexible, adaptable approach to manage changing business models and risks.

Disregard for Risk Results:

Risk assessment findings are not used to develop strategies or allocate resources.

Regularly assess and update ML/TF/PF risks to align with operations, customer types, and geographic scope.

Develop strategies and action plans based on risk assessment results.

Allocate sufficient resources to address identified risks.

Thank you