Preventing Circumvention: Practical Tips for Financial Institutions under CRS

Introduction

The Common Reporting Standard (CRS) was designed to promote tax transparency and ensure that financial account information is reported accurately across all jurisdictions. However, some individuals and entities attempt to avoid these obligations through practices known as "circumvention." Financial Institutions (FIs) play a critical role in detecting and preventing such practices, as failure to do so exposes them to regulatory, reputational, and financial risks. This advisory provides guidance on what constitutes circumvention, the anti-circumvention rules under the law, and the key measures FIs should adopt to strengthen compliance and safeguard their institutions.

What is Circumvention?

Under the CRS, *circumvention* means any action or inaction designed to, or resulting in, the avoidance of CRS reporting obligations.

Circumvention typically includes:

1. Structuring accounts or entities to fall outside CRS reporting, with the underlying objective of concealing reportable information. This involves deliberately arranging financial accounts or entities, so they appear exempt from CRS reporting requirements.

   For example:

   - Improperly using a Non-Reporting Financial Institution (Non-RFI), such as transferring assets into a pension fund or government-controlled entity not for legitimate purposes, but to avoid CRS reporting.
   - Interposing shell entities to disguise the identity of the true controlling person (beneficial owner).

2. Misrepresenting residency by relying on residence-by-investment /citizenship-by-investment schemes (CBI/RBI) or low-tax jurisdictions with minimal substance requirements.

3. Artificial arrangements where transactions or account ownership are set up solely to avoid CRS due diligence.

   For example: splitting accounts to stay below reporting thresholds or transferring assets to excluded products.

4. Providing false or misleading self-certifications to a financial institution.

5. Financial Institutions not applying CRS rules properly (knowingly or negligently) to attract clients seeking secrecy.

What is Anti-Circumvention?

Under the Mutual Administrative Assistance in Tax Matters Act, any person, including financial institutions, account holders, or financial advisors, who tries to avoid CRS reporting through any arrangement or practice, can be held responsible and remains subject to reporting obligations. In practice, a Financial Institution must treat any arrangement or practice entered into mainly to avoid CRS rules as "null and void". The "null-and-void" rule means that if a scheme to avoid CRS is detected, all reporting obligations still apply as if the scheme had not existed. In short, even if a client or FI attempts to disguise or reclassify an arrangement, the reporting obligation under CRS remains unchanged.

Anti-Circumvention Methods

1. Enhanced Onboarding Checks

- At account opening, always ensure you receive **valid CRS self-certification**.
- Cross-check the client's declared residency against **KYC/AML documents** (passport, proof of address, etc.).
- If residency looks suspicious (e.g., person uses a CBI/RBI "golden visa" but shows no real ties to that country), ask for **extra proof** (tax residency certificate, utility bill).
- **Note:** An FI must not rely on a self-certification if it has reason to doubt it.

2. Residency Verification

- Mis-stating residency is a **common circumvention tactic**.
- Financial Institutions should regularly scan internal records for "indicia" of other residencies (mailing addresses abroad, foreign phone numbers, instructions to transfer funds overseas, power of attorney abroad, "hold mail" requests, etc.).
- If such indicia are found, the account is treated as **reportable** for all jurisdictions that appear.
- Special care must be taken if a client suddenly presents a **new passport or tax ID from a low-tax country** – enhanced due diligence must be applied.

3. Controlling Person Checks (Beneficial Owners)

- Entities (companies, trusts, etc.) may hide reportable persons.
- Financial Institutions must "look through" the structure to identify **controlling persons** (natural persons behind entities).
- For trusts this includes **trustees, settlors, protectors, beneficiaries, or classes of beneficiaries, and anyone with ultimate control**; and for companies **the person who holds 25% or more of the shares** in the company.
- CRS checks cannot be skipped just because AML/KYC was weak, CRS requires full documentation of controlling persons.

4. Credentialing / Monitoring High-Risk Clients

- Clients seeking secrecy (from secrecy jurisdictions "tax havens", opening many small accounts, etc.) should face **enhanced scrutiny**.
- Systems should flag suspicious patterns (multiple linked accounts, moving money out of a reportable account and putting it into a product or account that is **excluded from CRS reporting**, fast movements of funds).

  Examples of a "product or account excluded from CRS":

  - Certain **retirement or pension accounts** under the CRS and MAATMA Regulations.
  - Some **low-risk life insurance contracts**.
  - Certain **escrow accounts** (like those used temporarily in a house purchase).
  - Certain **tax-favoured accounts** (like dormant accounts that do not exceed US1,000)
  - Accounts held by **governmental entities or international organizations**.

  These are excluded because they're considered **low risk for tax evasion**.

- Any **false, expired, or missing documents** must trigger immediate remediation.

How to Monitor and Control Accounts

1. Account Aggregation

- FIs may consider **adding up all accounts belonging to the same person** to see if they meet reporting thresholds. This would arise in cases where clients are trying to avoid reporting by splitting money into multiple small accounts.
- FI systems should automatically link accounts by:
  - Tax Identification Number (TIN),
  - Client ID,
  - Known relationships (family, business links),
  - Or knowledge from a relationship manager.

For example: Three USD 400k accounts when combined may produce USD 1.2 million, potentially making it a **High Value Account**.

2. Threshold and Transaction Alerts

- FIs should build threshold and transaction alerts into their systems to flag any potential avoidance or circumvention.

For example:

- Where several small accounts are closed and funds moved into a single new account. The client may try to "reset" their balances by moving money around so their accounts appear new and possibly escape detection, even though the overall funds should still be reportable.
- Where multiple accounts opened under the same person, each just below the CRS reporting threshold. Instead of keeping one large account that would clearly require reporting, a client may split their money across several smaller accounts so that each one looks too small to be reportable on its own.

- These alerts help identify **avoidance or circumvention schemes**.

3. Electronic Record Searches

- CRS requires FIs to check for **indicia of foreign residency** (foreign addresses, phone numbers, mailing instructions abroad, power of attorney abroad).
- FI systems can automate this by scanning existing account data.
- If indicia are found, the FI must:
  - Request a new valid self-certification, or
  - Treat the account as reportable for that jurisdiction.
- Automation ensures no indicia are missed due to human oversight.

Suggested Ways Forward

1. Documentation Reviews

- Officers should **sample accounts** and check the files.
- They need to confirm that:
  - Accounts have a **valid self-certification**.
  - All **AML/KYC documents** are there.
  - Any follow-ups (like proof of address requests, notes on why it's non-reportable, or escalation steps) are recorded.
- This makes sure FIs keep the **required records** showing they actually followed CRS due diligence.

2. Testing for Weaknesses

- Compliance should run **simulated tests** or "mystery shopping" exercises to see if systems or staff could be tricked.
- Examples:
  - Try splitting money into multiple accounts to see if the aggregation rule catches it.

    - Open two accounts under the same TIN and confirm the system combines them.
    - Submit a false residency claim to check if staff detect the problem.
- If weaknesses are found, the FI must fix them right away.

3. Compliance Reporting

- If internally you find **systemic problems** (like missing self-certs, or staff failing to check controlling persons), these must be reported.
- FIs may apply internal consequences, ranging from retraining to more serious disciplinary measures, in accordance with their policies.

  Compliance should maintain a **log of remediation actions** to prove the FI is actively working against circumvention and conducting due diligence.

Conclusion

Preventing circumvention protects both the integrity of Belize's tax system and the reputation of Financial Institutions. Effective implementation of CRS due diligence, continuous monitoring, and a culture of compliance are essential to ensure that reporting obligations are met and that Belize remains a trusted jurisdiction for transparent financial activity.