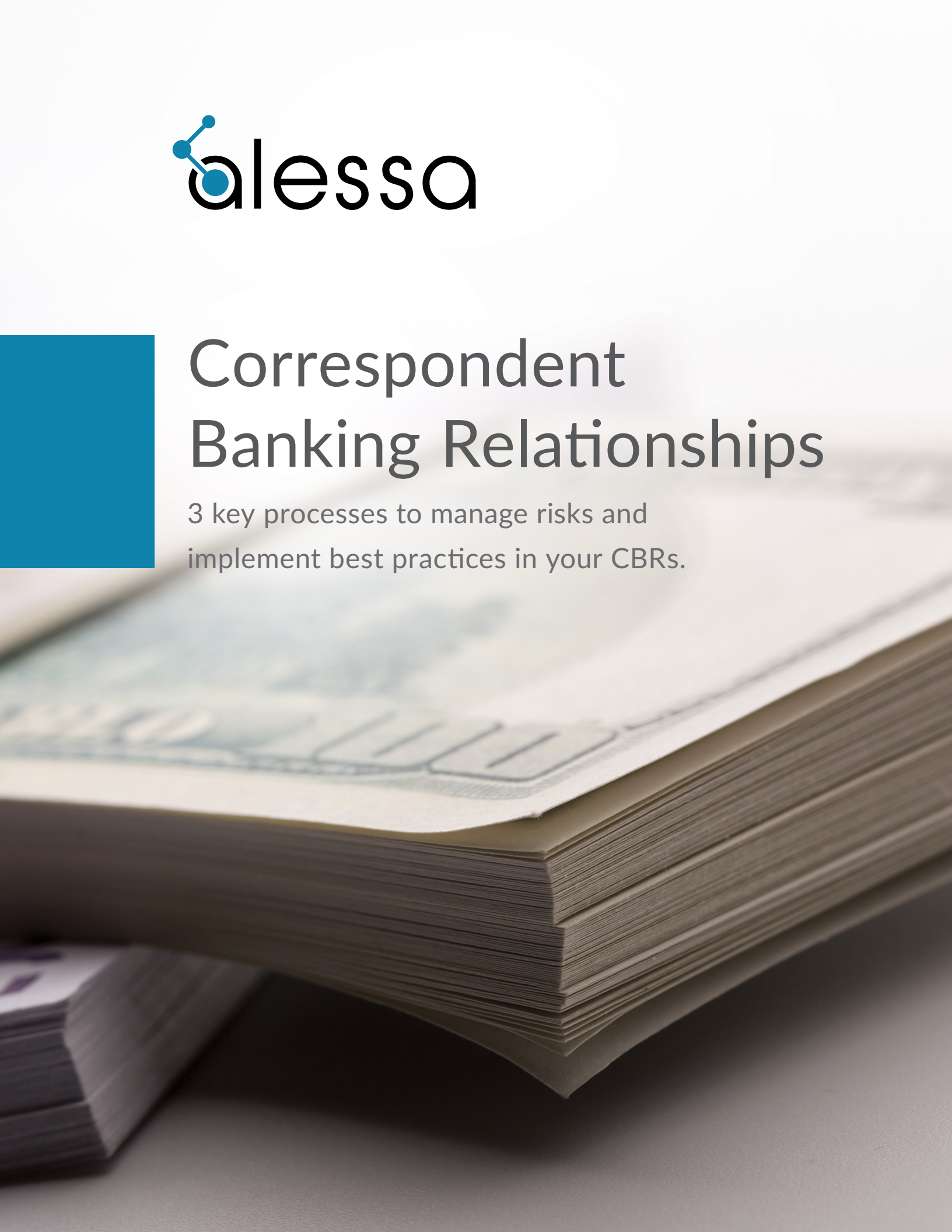
alessa

Correspondent Banking Relationships

3 key processes to manage risks and implement best practices in your CBRs.



> *"Prudent relationship management is only part of the solution. The sheer volume of transactions involved in correspondent banking will require financial institutions to explore a host of novel, data-driven surveillance strategies to identify the true bad actors who are subverting the system and marginalizing legitimate businesses and individuals."*
>
> *~PwC, Correspondence course: Charting a future for US-dollar clearing and correspondent banking through analytics*

A global trend is putting the financial systems of many small, developing areas of the world in jeopardy. Known as de-risking, the phenomenon has been growing for several years and is harming the countries and banks that are most dependent on correspondent banking relationships to access the international financial system.

Adding to the woes, increasing regulations and penalties for non-compliance is making correspondent banking relationships (CBRs) even more risky and complex.

The downside of de-risking

Because these relationships can pose significant risk, many correspondent banks are choosing to simply end their CBRs. The downside? Respondent banks are denied access to foreign currency and the international financial system at large, with many (particularly developing countries) being severely impacted.

In Belize, for example, only two financial institutions currently maintain CBRs with banks in the United States. Reduced access to the financial system has the potential to significantly grow the less-easily monitored informal methods of storing and transferring monies.

Those working in other areas of the Caribbean's financial industry have taken note—and have had to take steps to proactively protect their relationships.

Three must-have AML processes to save CBRs

It's simply not enough for respondent banks to meet just the minimum thresholds for compliance. To ensure they're not deemed to be risky, respondent banks have to continuously work on strengthening their anti-money laundering (AML) compliance programs.

By improving three key processes, respondent banks can make their compliance programs stronger and more robust, making their CBRs less likely to be cut as part of de-risking. This white paper will address these processes and provide concrete details on how respondent banks can adopt and utilize each of them.

Key process #1

Comprehensive onboarding

Because they don't have a direct relationship with the customer, correspondent banks rely on respondent banks to do thorough screening and follow proper KYC (know your customer) processes. This can include taking extra steps to validate customer identities; implementing a software solution to detect missing or incomplete customer data; and calculating and maintaining customer risk scores based on defined metrics that are updated as the customer's information or circumstances change.

Tighten minimum requirements

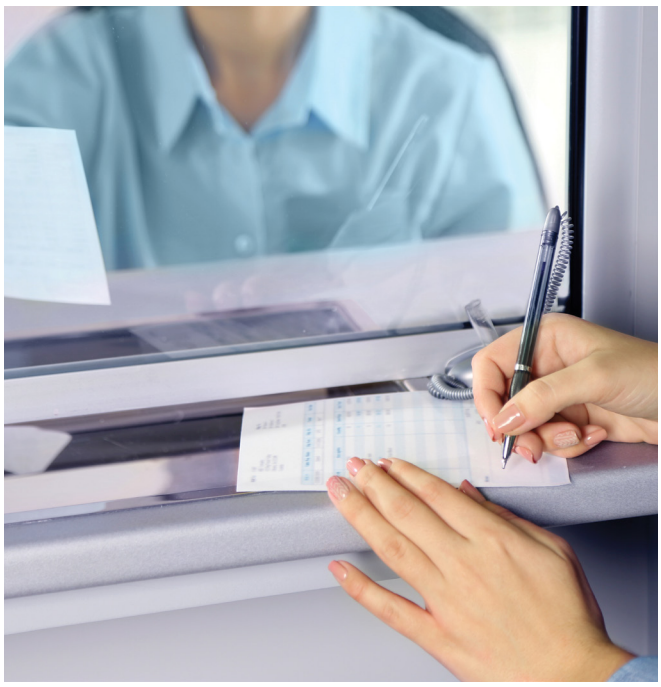
To go above and beyond basic compliance requirements, respondent institutions should collaborate with correspondent banks by pulling and reviewing data from utilities and other shared sources of customer data. They can also implement a process that is more stringent than may be required.

For example, although not required by law, as part of their customer due diligence activities banks could adopt the World Bank's recommendation to have customers submit a signed form declaring the identity and details of the ultimate beneficial owner of a business relationship or transaction. These declarations should be written to indicate that criminal penalties will follow for anyone found to have intentionally made a false statement on the form.

Tips from the field

Typically, correspondent banks require only confirmation rather than verification that enhanced due diligence (EDD) has been conducted for KYC. However, respondent banks must have a verification process in place, whether manual or electronic, to ensure that KYC data has been collected properly and without errors. Correspondent banks want to be made aware of issues identified during the KYC process, so respondent banks need to implement checks to ensure the accuracy of information collected.

The National Commercial Bank (NCB) in Jamaica, for example, has approached this challenge by designating separate staff to be responsible for collecting and verifying information about clients.



Examples of good practices for CBRs from the Qatar Financial Centre Regulatory Authority

The Qatar Financial Centre Regulatory Authority recently released a document to provide firms with guidance on general principles and best practices for correspondent banking services. Here are some examples of what they consider good practices.

Risk assessment of respondent banks

- Regular assessments of correspondent banking risks taking into account various risk factors such as the country; ownership and management structure; products and operations; transaction volumes; market segments; the quality of the respondent's AML systems and controls, and any adverse information known about the respondent.
- Risk scores that drive the frequency of relationship reviews.
- Consider publicly available information from government, non-governmental and other credible sources.

Ongoing monitoring of respondent accounts

- Review periods driven by the risk rating of a particular relationship, with high-risk relationships reviewed more frequently.
- Updating screening of respondents and connected individuals to identify individuals/entities with political connections (Politically Exposed Persons or PEPs) or on relevant sanctions lists.
- Involving senior management and AML staff in reviews of respondent relationships and consideration of whether to maintain or exit high-risk relationships.
- Where appropriate, using intelligence reports to help decide whether to maintain or exit a relationship.
- Carrying out ad-hoc reviews in light of material changes to the risk profile of a customer.

Customer onboarding

- Assigning clear responsibility for the customer due diligence (CDD) process and the gathering of relevant documentation.
- EDD for respondents that present greater risks or where there is less publicly available information about the respondent.
- Gathering enough information to understand customer details; ownership and management; products and offerings; transaction volumes and values; customer market segments; customer reputation; as well as the AML control environment.
- Screening the names of senior managers, owners and controllers of respondent banks to identify PEPs and assessing the risk that identified PEPs pose.
- Independent quality assurance work to ensure that CDD standards are up to required standards consistently across the bank.
- Discussing with overseas regulators and other relevant bodies the AML regime in a respondent's home country.
- Identifying risk in particular business areas (e.g., informal value transfer such as 'hawala', tax evasion, corruption) through discussions with overseas regulators.
- Visiting, or discuss with, respondent banks to discuss AML issues and gather CDD information.
- Gathering information about procedures at respondent firms for sanctions screening and identifying and managing PEPs.
- Understanding respondents' processes for monitoring account activity and reporting suspicious activity.
- Requesting details of how respondents manage their own CBRs.
- Senior management/committee sign-off for new CBRs and reviews of existing ones.

Key process #2

Determining ultimate beneficial ownership

Correspondent banks must know who the ultimate beneficiary of a customer or group is; however, this becomes more challenging as ownership structures grow more complex and multi-layered — sometimes done intentionally to conceal the identities of ultimate beneficial owners (UBOs) participating in illegal activities. In addition, any due diligence done by the correspondent bank is diluted as the distance between it and the ultimate beneficiary increases.

A winning strategy

One of the best ways for organizations to protect themselves when it comes to UBO is to have a comprehensive, risk-based process that helps identify the beneficial owners, and determines the risk they present to the company.

Once a risk has been identified, appropriate due diligence measures can be determined—that is, whether additional information needs to be obtained from sources beyond the customer—to ensure efforts are focused on high-risk areas. Ownership relationships can then be monitored regularly.

Real-life processes

Some correspondent banks wish UBO to be established below the 25% threshold recommended by the Financial Action Task Force (FATF). As part of some respondent banks' AML compliance requirements, due diligence checks are completed on all beneficiaries, as appropriate.

Ownership relationships are regularly monitored, including against external watch lists such as Refinitiv's World-Check database. In addition, some respondent banks, including NCB, have designed custom forms that must be completed to demonstrate that due diligence has been done to identify UBOs, specifically when conducting cross-border transactions.

In this situation, individuals must be screened, and the intermediary must identify on whose behalf the transaction is being done. Although in Jamaica, where ownership structures tend to be transparent, NCB recommends asking questions and seeking verification when the structures become complex and layered, especially if some of those layers involve persons in jurisdictions other than the one in where the relationship is established and/or maintained.

Although these measures are not yet universally required by law, they are an emerging practice that correspondent banks are interested in seeing. Proactive measures such as this are especially reassuring to correspondent banks as they demonstrate commitment to a strong AML compliance program.

The Wolfsberg - Correspondent Banking Due Diligence Questionnaire (CBDDQ)

In 2018, the Wolfsberg Group updated its Correspondent Banking Due Diligence Questionnaire (CBDDQ) and related guidance material. The aim of the CBDDQ is to set an enhanced and reasonable standard for cross-border and/or other higher risk Correspondent Banking Due Diligence. Below is a sample of some of the questions from the questionnaire.

Entity and ownership

- Full legal/business name, address
- Date of entity incorporation/establishment
- Type of ownership. If publicly traded, which stock exchanges where ordinary shares/common stock are primary listed.
- Is Entity more than 25% government or state-owned?

Anti bribery & anti corruption

- Has the Entity documented policies and procedures to (reasonably) prevent, detect and report bribery and corruption?
- Does the Entity have a policy that includes enhanced requirements regarding interaction with public officials?

Products and services

- Does the Entity offer correspondent banking services to domestic banks, allow domestic bank clients to provide downstream relationships or offer correspondent banking services to foreign Banks?
- What are the stored value instruments the Entity provides; e.g., prepaid cards, e-wallet, government benefit cards. Any other high-risk products and services?

Policies and procedures

- Are the Entity's policies and procedures gapped against/compared to U.S. and EU standards?
- Does the Entity have policies and procedures that prohibit opening and keeping of accounts for Section 311 designated entities?
- Specify how potentially suspicious activity identified by employees is to be escalated and investigated.

AML, CTF & sanctions programme

- Does the Entity have a programme that sets minimum AML, CTF and sanctions standards that include an appointed officer with sufficient experience/expertise, cash reporting, policies and procedures,risk assessment, training and education.
- How many full-time employees are in the Entity's AML, CTF and sanctions compliance programme?
- Does the Entity use third parties to carry out any part of its AML, CTF & Sanctions programme?

AML, CTF & sanctions risk assessment

- Does the Entity's AML & CTF enterprise-wide risk assessment (EWRA) cover the inherent risk components including client, product, channel, and geography?
- Does the entity's AML & CTF EWRA assess how well controls are operating?

KYC, CDD and EDD

- Does the Entity verify the identity of the customer?
- Does the Entity gather and retain the following when conducting CDD: expected activity, nature of business or employment, and product usage.

Key process #3

Screening cross-border transactions

When it comes to conducting cross-border transactions, respondent banks must demonstrate that they have thoroughly screened each transaction as well as screened for high-risk individuals and groups. Transactions should be screened in real-time to ensure that any non-compliant or suspicious transactions are intercepted before being sent to the correspondent bank for processing.

Going above and beyond

Respondent banks should consider adopting FATF's recommended standard for originator and beneficiary details in payment messages. This involves recording full originator and beneficiary information for all cross-border wire transfers, which serves to increase transparency and puts correspondent banks at ease.

Furthermore, transactions should also be monitored by an automated system to provide good quality assurance, an audit trail, and flag alerts to the compliance team so they can then be investigated and remediated.

Removing legal impediments

Privacy laws in some countries may prevent the transmission of additional information by the respondent bank to its correspondent bank concerning transactions, their originators and beneficiaries.

The International Monetary Fund (IMF) recommends exploring amendments to legal frameworks as one option to overcome these hurdles. In an example provided by the IMF, "the Mexican authorities have adopted regulations to remove previously existing legal barriers to information sharing arising from Mexico's banking secrecy laws and to permit domestic banks to share specific additional information on certain cross-border transactions with registered foreign correspondent banks".

In some cases, simply redrafting banking contracts is all that is needed to overcome the privacy barriers.

Strategies put into action

NCB uses an automated system that screens all parties and relevant transactions in real-time. The bank also requires that intermediaries identify on whose behalf the transaction is being conducted.

When the correspondent bank can see that the respondent bank is implementing solutions and taking steps to actively monitor transactions and groups, it is more likely to view the respondent bank as a trusted partner that can increase quality business—rather than put the correspondent at risk.

Conclusion: Securing relationships and moving forward

Small and medium-sized financial institutions must be able to access foreign currency and the global financial market through correspondent banking relationships. To avoid having these ties severed due to de-risking, respondent banks must take steps to ensure they pose the least risk possible to their correspondent banks.

Improving the three key processes identified in this white paper will not only protect CBRs —it will create a strong compliance program that will have significant benefits for the organization. Fines and penalties can be avoided, and moving forward a strengthened compliance program can also be leveraged in merger and acquisitions strategies as part of a de-risking response.

About CaseWare RCM

CaseWare RCM Inc. is the maker of Alessa, a financial crime detection, prevention and management solution. With deployments in more than 20 countries in banking, insurance, FinTech, gaming, manufacturing, retail and more, Alessa is the only platform organizations need to identify high-risk activities and stay ahead of compliance. To learn more about how Alessa can help your organization ensure compliance, detect complex fraud schemes, and prevent waste, abuse and misuse, visit us at **www.alessa.com.**


150 Isabella Street, Suite 800
Ottawa, ON K1S 1V7, Canada


1-844-265-2508


alessa@caseware.com


www.alessa.com

alessa