ARCTIC INTELLIGENCE

Compliance. The smart way.

Correspondent Banking AML/CTF & Sanctions Risk Domain

Fact Sheet

WHAT IS CORRESPONDENT BANKING?

Correspondent banking is a financial arrangement between two banks, usually from different countries, where one bank (the correspondent bank) provides services on behalf of another bank (the respondent bank). These services often involve facilitating international transactions, processing payments, and managing foreign currency exchanges. Correspondent banking helps smaller or less established banks gain access to global financial networks and services, allowing them to conduct cross-border transactions and provide international banking services to their customers.

Why conduct a correspondent banking risk assessment?

Compliance with Regulations

Regulatory authorities, such as financial crime enforcement agencies and international bodies, require financial institutions to have effective risk assessment and risk management processes in place for correspondent banking relationships. Failing to comply can lead to regulatory penalties and reputational damage.

Preventing Financial Crime

Correspondent banking relationships can be exploited for money laundering, terrorist financing, and other illicit activities. By conducting risk assessments, you can identify potential risks and take steps to prevent these activities from occurring within your banking network.

Maintaining Reputation

Involvement in any form of financial crime, even unwittingly, can seriously damage a bank's reputation. Conducting risk assessments demonstrates your commitment to ethical and responsible banking practices, which can help maintain trust among customers, regulators, and partners.

Risk Management

Risk assessments enable you to identify higher-risk relationships and transactions. This allows you to implement appropriate risk mitigation measures, such as enhanced due diligence, ongoing monitoring, and reporting suspicious activities.

Avoiding Financial Losses

Engaging with high-risk respondent banks without proper risk assessment can lead to financial losses, legal liabilities, and potential disruptions to your own operations.

Protecting the Financial System

The global financial system's stability relies on the integrity of correspondent banking relationships. By conducting risk assessments, you contribute to safeguarding the system from abuse and illicit activities.

Adherence to Best Practices

Risk assessments help you adhere to industry best practices for risk management in correspondent banking. This can improve your institution's overall operational efficiency and effectiveness.

Strengthening Due Diligence

A thorough risk assessment process involves gathering comprehensive information about respondent banks, helping you better understand their business operations, customers, and compliance practices.

Regulatory Reporting

Many jurisdictions require banks to report suspicious transactions or activities. A well-conducted risk assessment can help you identify such activities and fulfil reporting obligations.

Legal Compliance

Depending on the jurisdiction, failure to adequately assess correspondent banking risks could result in legal consequences, including fines, sanctions, or legal actions.

CONDUCTING A CORRESPONDENT BANKING RISK ASSESSMENT IN

12 STEPS

STEP 01

Identify and Gather Information: Collect relevant information about each respondent bank, including ownership structure, location, business activities, and customers. Obtain information about the regulatory environment in the respondent bank's country.

STEP 02

Risk Categorisation: Categorise your correspondent banking relationships based on risk levels. Consider factors like the respondent bank's location, regulatory environment, AML/CTF controls, and transaction patterns.

STEP 03

Risk Assessment: Evaluate the risks associated with each correspondent banking relationship. Consider the inherent risks (geographical, regulatory, etc.) and the controls the respondent bank has in place to mitigate those risks.

STEP 04

Enhanced Due Diligence (EDD): For higher-risk relationships, apply enhanced due diligence measures. This may involve conducting more detailed investigations, requesting additional documentation, and verifying the source of funds.

STEP 05

Sanctions and PEP Screening: Screen respondent banks and their customers against sanctions lists and lists of politically exposed persons (PEPs) to ensure compliance with international sanctions and anti-corruption measures.

STEP 06

Ongoing Monitoring: Implement ongoing monitoring of correspondent banking relationships and transactions to detect any suspicious activities or patterns.

STEP 07

Documentation: Document all steps taken during the risk assessment process, including findings, decisions, and actions taken to mitigate risks.

STEP 08

Risk Mitigation: Implement appropriate risk mitigation measures for each relationship. This could include adjusting transaction limits, applying transaction monitoring systems, and conducting periodic reviews.

STEP 09

Internal Reporting: Maintain clear channels of communication with internal compliance teams and management regarding risk assessment findings, potential issues, and mitigation strategies.

STEP 10

Reporting Suspicious Activities: If you identify any suspicious transactions or activities, report them to the relevant regulatory authorities in accordance with regulatory requirements.

STEP 09

Regular Reviews and Updates: Conduct regular reviews of your correspondent banking relationships and risk assessments. Update risk assessments whenever there are significant changes to a respondent bank's operations or regulatory environment.

STEP 10

Training and Awareness: Ensure that your staff members are trained to understand and follow your correspondent banking risk assessment procedures and policies.

About Arctic Intelligence

Arctic Intelligence (www.arctic-intelligence.com) is a multi-award winning, RegTech firm that specialises in audit, risk and compliance software related to financial crime compliance and risk management. Arctic Intelligence has helped hundreds of large and small clients across over 20 industry sectors and 20 countries and has also developed strong industry partnerships around the world.

Arctic has developed two leading cloud-based software solutions that leverage technology to re-engineer the way in which major financial institutions and other regulated businesses manage their enterprise-wide financial crime and non-financial crime risks.

VISIT OUR WEBSITE

BOOK A DEMO TODAY

APAC

Arctic Intelligence Head Office
Level 4, 11-17 York Street,
Sydney, NSW 2000,
Australia

Call us on your local number:
Australia +61 (0) 2 8001 6433
New Zealand +64 (0) 9889 9825
Singapore +65 6817 8650

EMEA

United Kingdom +44 20 8157 0122

AMERICAS

USA +1 917 730 4484
Canada +1 613 518 8002

GLOBAL

support@arctic-intelligence.com

ARCTIC INTELLIGENCE

Compliance. The smart way.