

Disclaimer: This document has been converted to reference Axum and Curaçao jurisdictional terms (Curaçao Gaming Authority - CGA, FIU Curaçao, LOK, NORUT). Legal citations must be reviewed by Curaçao counsel.

| Version | Date       | Description             | Updated By  | Approved |
|---------|------------|-------------------------|-------------|----------|
| v.1     | 28/10/2025 | Compliance & AML Manual | Keivana Lee |          |
|         |            |                         |             |          |

## Contents

|                                                                                                               |    |
|---------------------------------------------------------------------------------------------------------------|----|
| CHAPTER 1: INTRODUCTION.....                                                                                  | 1  |
| 1.1 AXUM Policy Financial Crime Prevention .....                                                              | 1  |
| 1.2 Financial Crime Risk .....                                                                                | 2  |
| 1.3 Law, Regulation and Industry Practice .....                                                               | 2  |
| 1.4 General Principles .....                                                                                  | 4  |
| CHAPTER 2: OVERVIEW OF MONEY LAUNDERING AND TERRORISM FINANCE .....                                           | 5  |
| CHAPTER 3: AML POLICY AND PROGRAM GUIDELINES.....                                                             | 6  |
| 3.1 Registration .....                                                                                        | 6  |
| 3.2 Resident Compliance Officer Designation and Duties .....                                                  | 6  |
| 3.3 Risk Assessment.....                                                                                      | 7  |
| 3.4 Training .....                                                                                            | 8  |
| 3.5 Sharing AML Information with International Law Enforcement Agencies and Other Financial Institutions..... | 9  |
| CHAPTER 4: OFFENCES.....                                                                                      | 12 |
| 4.1 Introduction .....                                                                                        | 12 |
| 4.2 Penal Code of Curaçao (Wetboek van Strafrecht) .....                                                      | 12 |
| 4.3 Landsverordening identificatie bij dienstverlening (LID).....                                             | 15 |
| 4.5 LOK (Landsverordening op de Kansspelen) .....                                                             | 15 |
| CHAPTER 5: INTERNAL COMMUNICATIONS .....                                                                      | 16 |
| 5.1 Money Laundering Reporting Officer .....                                                                  | 16 |
| 5.2 Contact with Third Parties .....                                                                          | 17 |
| 5.3 Orders .....                                                                                              | 17 |
| CHAPTER 6: THE RISK BASED APPROACH.....                                                                       | 18 |
| 6.1 Introduction .....                                                                                        | 18 |
| 6.2 Risk Potential .....                                                                                      | 18 |
| 6.3 Evaluating the Risk to AXUM.....                                                                          | 19 |
| 6.4 Client Risk Assessment.....                                                                               | 20 |
| CHAPTER 7: CLIENT DUE DILIGENCE PROCEDURE .....                                                               | 20 |
| 7.1 Introduction .....                                                                                        | 20 |
| 7.2 What is CDD? .....                                                                                        | 21 |
| 7.3 Timing of, and non-compliance with, CDD measures .....                                                    | 21 |
| 7.4 Application of CDD Measures.....                                                                          | 21 |
| 7.5 Who is the Client? .....                                                                                  | 22 |
| 7.6 Who is the Beneficial Owner?.....                                                                         | 22 |
| 7.7 Existing Clients.....                                                                                     | 22 |
| 7.8 Construction of an Economic Profile.....                                                                  | 22 |
| 7.9 Simplified Due Diligence.....                                                                             | 23 |
| 7.10 Enhanced Due Diligence .....                                                                             | 23 |

|                                                               |    |
|---------------------------------------------------------------|----|
| 7.11 Exception to Full Identification .....                   | 24 |
| 7.12 Standard of Verification Evidence.....                   | 24 |
| 7.13 Prohibited Business Activities.....                      | 28 |
| CHAPTER 8: IDENTIFICATION EVIDENCE AND KYC .....              | 29 |
| 8.1 Introduction .....                                        | 29 |
| 8.3 Clients Subject to Full Identification Requirements ..... | 31 |
| 8.4 Natural Persons.....                                      | 32 |
| 8.5 Unregulated Private Companies.....                        | 34 |
| 8.6 Partnerships and Unincorporated Businesses .....          | 35 |
| 8.7 Limited Partnerships.....                                 | 36 |
| 8.8 Non-Government and Public Authorities.....                | 36 |
| 8.9 Politically Exposed Persons ('PEPs').....                 | 38 |
| CHAPTER 9: OUTSOURCING .....                                  | 41 |
| 9.1 Regulatory Requirement.....                               | 41 |
| 9.2 Materiality.....                                          | 41 |
| 9.3 Evaluation of Outsourcing Risk .....                      | 42 |
| CHAPTER 10: SUSPICIOUS TRANSACTIONS .....                     | 43 |
| 10.1 Internal Reporting.....                                  | 43 |
| 10.2 Suspicious Activity Reporting and Related Matters.....   | 46 |
| 10.3 Examples of Suspicious Activity .....                    | 47 |
| 10.4 Responding to Red Flags and Suspicious Activity .....    | 47 |
| 10.5 Ongoing Relationships with Suspicious Clients .....      | 52 |
| 10.6 Record Keeping.....                                      | 52 |
| CHAPTER 11: MONITORING.....                                   | 52 |
| 11.1 Introduction .....                                       | 53 |
| 11.2 Up-To-Date Client Information.....                       | 53 |
| 11.3 Transaction Monitoring .....                             | 53 |
| 11.4 Funds Transfer and Travel Rule Compliance.....           | 54 |
| 11.5 Record Keeping.....                                      | 54 |
| CHAPTER 12: RECORD RETENTION .....                            | 54 |
| 12.1 Introduction .....                                       | 54 |
| 12.2 What records have to be kept?.....                       | 55 |
| 12.3 Identification Records .....                             | 55 |
| 12.4 Transaction Records .....                                | 55 |
| 12.5 Third party Record Keeping.....                          | 55 |
| 12.6 Internal and External Suspicious Activity Reports.....   | 55 |
| 12.7 Anti-Money Laundering Training Records.....              | 56 |
| 12.8 Compliance Monitoring Records.....                       | 56 |
| 12.9 Refused Business Records .....                           | 56 |
| 12.10 Wire Transfer and Electronic Payment Records .....      | 56 |
| 12.11 Format and Retrieval of Records .....                   | 56 |
| 12.12 Sanctions and Penalties .....                           | 57 |
| Chapter 13: SANCTIONS .....                                   | 57 |

|                                                                                  |    |
|----------------------------------------------------------------------------------|----|
| 13.1 Introduction .....                                                          | 57 |
| 13.2 Policy Statement .....                                                      | 58 |
| 13.3 Sanctions Programs .....                                                    | 59 |
| 13.4 Jurisdictions Subject to Comprehensive Embargoes .....                      | 60 |
| 13.5 Facilitation .....                                                          | 60 |
| 13.6 No Grandfathering.....                                                      | 61 |
| 13.7 Compliance Procedures .....                                                 | 61 |
| 13.8 Identifying Sanctions Compliance Risk.....                                  | 61 |
| 13.9 Licences.....                                                               | 62 |
| 13.9.1 General Licences .....                                                    | 62 |
| 13.9.2 Specific Licenses.....                                                    | 62 |
| 13.10 Reports and Records.....                                                   | 63 |
| 13.12 Training .....                                                             | 63 |
| 13.13 Responsible Individual.....                                                | 63 |
| 13.14 Sanctions Violations .....                                                 | 63 |
| 13.15 Handling Blocker Property and Rejected Transactions .....                  | 64 |
| CHAPTER 14: Governance and Oversight                                             |    |
| 14.1 Senior Management Responsibilities and Governance .....                     | 65 |
| APPENDIX 1: SUSPICIOUS TRANSACTION REPORTING (STR) FORM (MONEY LAUNDERING) ..... |    |
| APPENDIX 2: AML COURSE REGISTER OF ATTENDEES .....                               | 64 |
| APPENDIX 3: PROOF DOCUMENTS FOR NATURAL PERSONS .....                            | 65 |
| APPENDIX 4: SAMPLE RED FLAGS .....                                               | 66 |
| APPENDIX 5: USEFUL INFORMATION SOURCES.....                                      | 68 |
| APPENDIX 6: SUMMARY OF EXISTING LAWS .....                                       | 72 |
| APPENDIX 7: ANTI-MONEY LAUNDERING MANUAL DECLARATION.....                        | 78 |
| APPENDIX 8: ENHANCED DUE DILIGENCE REPORT FOR AML PURPOSES.....                  | 78 |
|                                                                                  | 79 |

## CHAPTER 1: INTRODUCTION

### 1.1 Axum Policy Financial Crime Prevention

Axum. (hereafter the “Company” or the “Firm”, or “Axum”) incorporated under the laws of Curaçao, is committed to maintaining effective prevention and detection measures to assist the law enforcement authorities in combating financial crime. This Manual sets out the policies and procedures which have been adopted to meet the Firm’s legal obligations under Curaçao’s Anti-Money Laundering and Counter Terrorist Funding legislation.

These policies and procedures have been adopted by the Board of Axum and must be adhered to at all times.

Axum seeks to ensure at all times that:

- Clients’ identities are satisfactorily verified in accordance with the firm’s risk-based approach before the Company undertakes business with them;
- The Company knows its clients and understands their reasons for doing business with us both at the client acceptance stage and throughout the business relationship;
- Axum employees are trained and made aware of both their personal legal obligations and the legal obligations of the Company;
- Employees are trained to be vigilant for activities where there are reasonable grounds for suspicion that money laundering could be taking place and to make the reports to the Resident Compliance Officer(RCO) / MLRO; and,
- Sufficient records are retained for the required retention period.

We establish, maintain and implement appropriate procedures to achieve these objectives. Money laundering and fraud threats are dynamic and criminals constantly devise new techniques and exploit the easiest targets in the financial services sector. To mitigate the risk of being used as a vehicle for financial crime, Axum will systematically assess, mitigate, and monitor these risks. It will seek to identify fraud and money laundering at an early stage of the client acceptance process, escalate this to the Resident Compliance Officer (RCO) / MLRO and take appropriate action.

A risk-based approach adopted by the Company, is the driver of our overall strategy of fighting financial crime. Through this approach, we identify the areas of greatest vulnerability and focus our resources on those areas. Ultimate responsibility for this approach lies with the senior management but all employees carry a responsibility to maintain the effectiveness of systems and controls employed by the Company.

Given the nature of risks involved it is not possible to cover every possible eventuality in this Manual. Should an issue arise that is not specifically covered in this Manual, employees should refer to the Resident Compliance Officer(RCO) / MLRO for further guidance.

Although the platform does not currently permit virtual-asset payments, management recognises the emerging AML/CFT risks associated with crypto-enabled gaming. These are monitored under the Business Risk Assessment framework, referencing industry typology for virtual assets. Should the business model change, a specific Crypto-Asset Risk Assessment will be activated and submitted to the MLRO for approval.

This Program applies to all AXUM directors, officers, employees, and contractors regardless of their geographic location ("Covered Persons"). Covered Persons found to be in violation of this Program are subject to disciplinary action up to and including dismissal. Such persons may also be subject to civil or criminal penalties under applicable law.

## 1.2 Financial Crime Risk

The regulator's financial crime objective encompasses the prevention of financial fraud, market abuse and money laundering. Money laundering is the process by which criminals attempt to hide and disguise the true origin and ownership of the proceeds of their criminal activities, thereby avoiding prosecution, conviction and confiscation of criminal funds.

Money laundering and terrorist financing risks are closely related to the risks of fraud and insider dealing. While these are separate offences, money laundering involves handling the proceeds of any crime, including the proceeds of these activities.

The ability to launder the Curaçao AML/CTF legal framework through the financial system is vital to the success of criminal operations. But firms that become involved in money laundering risk prosecution or regulatory enforcement sanctions which potentially damage their reputation or brand.

To reduce the incidence of financial crime, the procedures that Axum has adopted focus on knowing our clients, understanding their businesses, carrying out proportionate verification checks, and identifying and reporting suspicious activity.

### 1.3 Law, Regulation and Industry Practice

As noted above, Axum is required to comply with international financial regulatory standards, including Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) regulations, by virtue of its operations as an online gaming platform across various global jurisdictions.

The Company and unregulated persons and entities alike are subject to various criminal money laundering statutes, which generally prohibit engaging in transactions that facilitate “laundering” of funds derived from certain criminal activities, or which facilitate the financing of terrorists and terrorism activity.

The international legal framework prohibiting the facilitation of money laundering is governed by various global and regional regulations, including but not limited to the recommendations of the Financial Action Task Force (FATF). In general, these regulations make it a criminal offense to knowingly engage in financial transactions or monetary transactions that involve the proceeds of specified unlawful activities, as defined under each jurisdiction's laws.

#### Anti-Money Laundering Requirements

In addition to general anti-money laundering laws applicable worldwide, online gaming platforms operating internationally are subject to additional obligations pursuant to the regulatory standards of the countries in which they operate. This includes compliance with international guidelines such as those set by the Financial Action Task Force (FATF) and regional regulatory bodies. Axum must adhere to registration and compliance requirements in each jurisdiction, implementing effective AML programs. These programs are designed to prevent the Axum and its products and services from being used to

facilitate money laundering and the financing of terrorist activities. They also aim to prevent Axum from accepting funds derived from unlawful activities or from sanctioned persons and entities. The AML Program should be commensurate with the risks posed by the Axums location, customer base, and the size, complexity, nature, and volume of the financial services provided.

This Program outlines the Company's policy and plans for adhering to these international requirements. The AML Program, along with related procedures and internal controls, are designed to ensure compliance with global anti-money laundering standards, applicable regional regulations, and economic sanctions laws. The Program will be regularly reviewed and updated by the Resident Compliance Officer to ensure it remains effective and compliant with both changes in international laws and the evolving nature of the Company's business.

Axum is subject to the laws of Curaçao and rules set by the Curaçao Monetary Authority (CGA). The CGA provides practical interpretation of legal and regulatory requirements and indicates good industry practice. The Firm has taken these laws and guidelines into account when devising a risk-based approach to the prevention of money laundering.

The laws of Curaçao specifically concerning money laundering and terrorist financing is contained in the following legislation:

- Penal Code of Curaçao (Wetboek van Strafrecht) – Articles 430b–430d (money-laundering offences).
- Landsverordening identificatie bij dienstverlening (LID), PB 2017 no. 92 – customer identification and verification.
- Landsverordening melding ongebruikelijke transacties (LMOT / NORUT), PB 2017 no. 99 – reporting of unusual transactions and tipping-off prohibitions.
- Landsverordening op de Kansspelen (LOK) – gaming operations and AML/CFT compliance obligations.
- Sanctions National Ordinance (N.G. 2014 no. 55) and Kingdom Sanctions Act (N.G. 2016 no. 54) – targeted financial sanctions.

#### 1.4 General Principles

In order to comply with the laws, regulations and guidance, the Company adopts the following principles:

### Money Laundering Reporting Officer

The Resident Compliance Officer(RCO) / MLRO acts as the central point of contact both with the Financial Intelligence Unit Curaçao (FIU Curaçao) (“FIU Curaçao”), law enforcement agencies and internally, in relation to all matters relating to money laundering. The Resident Compliance Officer(RCO) / MLRO monitors Axum’ compliance with the Company’s anti-money laundering procedures and submits reports to the Board at least on a quarterly basis. The Resident Compliance Officer(RCO) / MLRO is an approved person under the regulator’s Approved Persons regime.

### Risk-based Approach

The Firm has implemented policies, procedures and controls aimed at deterring criminals from using Axum for the laundering of Curaçao AML/CTF legal framework. These policies and procedures are tailored to the risk posed by individual clients, in accordance with the SIR.

### Client Identity Verification

Axum has established Client Due Diligence (“CDD”) procedures to identify the users of its services and, in relation to higher-risk clients, the principal beneficial owners and origins of funds. These procedures include knowing the nature of our clients’ businesses and being alert to abnormal transactions. Axum uses transaction velocity monitoring and social graph monitoring to raise flags when clients act out of pattern.

### Suspicious Transactions

Unexplained or abnormal transactions or activities that are suspected of being linked to criminal activity should be reported to the Resident Compliance Officer(RCO) / MLRO in writing without delay using the Suspicious Transaction Reporting Form (AML Form). The Resident Compliance Officer(RCO) / MLRO will determine whether to report the suspicions to the regulator. If the Resident Compliance Officer(RCO) / MLRO is absent, reports should be made to the company Chief Executive Officer. An acknowledgment of receipt should be obtained from the Resident Compliance Officer(RCO) / MLRO for every such report.

## Record-Keeping

Axum keeps records of who has been trained and the timing and form of training sessions. The Company is required by legislation to retain all records verifying the identity of our clients for at least seven years following the end of the business relationship. We also retain the records of any internal reports of suspicion submitted to the Resident Compliance Officer(RCO) / MLRO and any disclosures made to the regulator.

## Training

All employees must be informed of their individual and collective responsibilities and the Company's money laundering policies. Personnel are provided with training to enable them to understand the vulnerabilities of the business and to recognise and report suspicious activities.

## CHAPTER 2: OVERVIEW OF MONEY LAUNDERING AND TERRORISM FINANCE

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders, traveler's checks, or virtual currencies, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

Terrorist financing may or may not involve the proceeds of criminal conduct, but may nonetheless involve an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to launder funds.

## CHAPTER 3: AML POLICY AND PROGRAM GUIDELINES

### 3.1 Registration

Axum operates as a remote gaming operator under Curaçao's National Ordinance on Games of Chance (LOK) and is licensed/supervised by the Curaçao Gaming Authority (CGA). All licence applications and regulatory submissions are made via the CGA's online License Management Portal. Where Axum also provides platform/aggregation services to third parties, those activities fall under the B2B supplier category. Axum will migrate from any legacy authorisations to direct CGA licensing within the LOK transition timelines. Axum only offers services in jurisdictions where doing so is lawful and applies geoblocking/market exclusions where local licences are required or prohibitions apply. Axum maintains AML/CFT controls, KYC/age verification, sanctions screening, responsible-gambling measures, and reporting consistent with CGA requirements and relevant local laws.

The Resident Compliance Officer is responsible for ensuring that Axum adheres to these registration requirements in all jurisdictions of operation. This includes maintaining complete and accurate registrations, renewing them as required, and monitoring any changes in the business that might necessitate re-registration or notification.

To ensure timely renewal of registrations, the Resident Compliance Officers should set calendar alerts well in advance of the renewal deadlines, allowing sufficient time for the completion and submission of any required documentation. A best practice would be to aim for submission of renewals at least 30 prior to the deadline, adjusting the timeline according to the specific requirements of each jurisdiction.

### 3.2 Resident Compliance Officer Designation and Duties

The Company designates [ ] as the Resident Compliance Officer, who is part of the managerial team and covers Resident Compliance Officer(RCO) / MLRO Duties. The Resident Compliance Officer is vested with full responsibility and authority to enforce the Company's AML Program and has been appointed to that role by a resolution of the Axum board of directors. The duties of the Resident Compliance Officer are set forth in this Policy, and include:

- Risk Assessment. Periodically assessing the level of money laundering risks faced by the Company as a result of its business activities, customers, and geographic areas served (“Risk Assessment”).
- Training. Ensuring all Covered Persons whose duties are impacted by AML risk, including the risk identified in the Risk Assessment, are adequately trained to implement this Program as it pertains to their day-to-day activities. AML/CFT training requirements will apply to all individuals working within the Company, including those in temporary, contract, and part-time roles. The Resident Compliance Officer will ensure that these individuals receive the same level of training as full-time employees to guarantee uniform compliance with AML/ATF regulations.
- Employee Screening Prior to Hiring: The Company will implement pre-employment screening procedures to ensure that all prospective employees meet high standards of integrity and professional competence. This includes background checks, reference verification, and sanctions screening prior to hiring.
- Reporting and Record Retention. Ensuring that the Company keeps and maintains all of the required AML records and ensuring that any information regarding suspicious activity will be maintained for potential SAR filing.
- Program Updates. Ensuring that this Program and related compliance procedures are updated as necessary to reflect current requirements of applicable law and results of the Risk Assessment.
- Suspicious Activity Investigation. Ensuring that all suspicious activity is properly investigated and, where appropriate, reported on behalf of the Company.
- Independent Review. Ensuring that the Company’s compliance with this Program and applicable law is the subject of periodic, independent review.
- Implement Corrective Action. Ensuring that any deficiencies, findings, or recommendations resulting from periodic reviews or otherwise are properly addressed in a timely manner.
- Vendor Management. As applicable, ensuring that any third-party service provider (“Vendor”) to which the Company has delegated tasks related to this Program has adopted and implemented its own compliance policies and procedures that are appropriately designed to address the compliance risks inherent to the services provided and which are commensurate with the nature and complexity of the services provided.

The Company’s officers and directors shall ensure that the Resident Compliance Officer has adequate resources to complete the responsibilities listed in this Program. The Resident Compliance Officer is empowered to escalate AML compliance issues directly to the Company’s general counsel or outside counsel (“Company Counsel”), other executive management, and the board of directors, as appropriate.

### 3.3 Risk Assessment

The Company will conduct periodic Risk Assessments designed to evaluate the extent of the AML risk arising from the Company's activities for use by the Company to implement compliance controls to reduce the risks identified in the Risk Assessment. The Risk Assessment shall be reviewed and updated annually or more frequently as the Resident Compliance Officer deems appropriate under the circumstances, including with reference to any applicable legal requirements.

To determine the AML risk, the Risk Assessment considers the interaction of two broad sets of factors: (1) the inherent risks in a particular line of business or the Company as a whole; and (2) the quality of controls implemented by the Company to manage and mitigate those risks. The Risk Assessment should be used to determine whether the inherent risks identified are adequately addressed by the compliance controls, and identify compliance "gaps," i.e. inherent risks which are not addressed by existing controls.

If the Risk Assessment identifies any gaps, the Resident Compliance Officer will engage in further analysis to determine the additional controls that can be implemented to appropriately address these gaps. The Compliance Officer, with the assistance of the business line and other personnel as may be appropriate, will create an action plan to implement these additional controls, and test the effectiveness of the controls in addressing the gap.

### 3.4 Training

The Company will develop Covered Person training under the leadership of the Resident Compliance Officer on the BSA and other laws and regulations within the scope of this Program, the content of this Program, and procedures used to implement this Program.

The training will include, at a minimum: (1) how to identify red flags and signs of money laundering that arise during the course of the Covered Persons' duties ("Red Flags"); (2) what to do once the risk is identified (including how, when, and to whom to escalate unusual activity or other Red Flags for analysis); (3) what Covered Persons' roles are in the Company's compliance efforts and how to perform them; (4) the Company's record retention policy; and (5) the disciplinary consequences (including civil and criminal penalties) for non-compliance with applicable laws.

The Company may utilize a third-party service provider to deliver this training to Covered Persons. The Company will maintain records to show the persons trained, the dates of training, and the subject matter of their training.

Training will be conducted annually, or more frequently as the Resident Compliance Officer may decide is appropriate. The Company will review its operations to analyze whether certain Covered Persons, based on their assigned obligations, require additional specialized training. All new Covered Persons will be required to attend training upon hire, and periodically thereafter, as determined by the Compliance Officer. The Resident Compliance Officer is responsible for coordinating with the Company's management to ensure the appropriate AML training is conducted and will be responsible for making any subsequent changes or amendments to the Company's AML training program, as necessary. The Resident Compliance Officer shall provide specialized training to the Company's officers and directors at least annually.

Completion of training will be evidenced in a tracker that documents at least the following: 1) date of training; 2) name of the instructor; 3) method of delivery; 4) names of personnel who have completed the training; and 5) copy of the training content. See a sample Training Completion Tracker in Exhibit A attached hereto.

### 3.5 Sharing AML Information with International Law Enforcement Agencies and Other Financial Institutions

**Regulatory Requests.** If the Company receives a regulatory request concerning accounts and transactions from international regulatory authorities or law enforcement agencies, the Company will review and respond to the request. The Resident Compliance Officer is responsible for ensuring a timely and comprehensive response to all such requests. All requests and responses will be kept strictly confidential and stored electronically in a secure database with access strictly controlled by the Compliance Officer. The Resident Compliance Officer may consult with company counsel on these matters as needed.

**Procedures for Responding to International Regulatory Requests.** Upon receiving an information request from a regulatory authority, the Company will designate a point of contact, typically the Resident Compliance Officer or a deputy, to handle the request. The designated person will promptly search the Company's records to determine whether we maintain or have maintained any account for, or have engaged in any transaction with, each individual, entity, or organization named in the request.

The Company is required to search current accounts, accounts maintained by a named subject during a specified period, and transactions conducted during a specified period as outlined in the request. If a match is found, the Company will report it to the requesting authority using the prescribed format and method.

If no matching account or transaction is found, the Company will not reply to the request. The Company will not disclose the fact that an international regulatory agency has requested or obtained information, except as necessary to comply with the information request. The Company will protect the security and confidentiality of these requests and comply with applicable privacy laws.

The Company will direct any questions about the request to the requesting law enforcement agency or regulatory authority. Unless otherwise stated in the request, the Company will not be required to treat the information request as continuing in nature and will use the information only for purposes specified by the regulatory authority.

#### International Law Enforcement Requests

International law enforcement requests are official investigative demands issued by law enforcement authorities in various countries to obtain financial records from financial institutions. These requests are typically issued for purposes of counterintelligence, counterterrorism investigations, or other law enforcement purposes. No financial institution or officer, Covered Person, or agent of the institution can disclose to any person that a government authority has sought or obtained access to records through such a law enforcement request.

The Company will maintain the highly confidential nature of these requests. A request issued to the Company will be handled by the Compliance Officer. If any Covered Person receives a copy of the request, the recipient must promptly notify the Compliance Officer. To maintain the confidentiality of the records request, the Resident Compliance Officer of the Company will work with select Covered Persons and limit the disclosure of the source of the request. The Resident Compliance Officer will maintain the only copy of the request, and copies of all documents provided to the issuer of the request. All related files will be kept electronically in a database with access strictly limited by the Compliance Officer.

Receipt of such a law enforcement request does not, by itself, require the filing of a Suspicious Activity Report (SAR). The Compliance Officer, or designee, will conduct an investigation and assess the information to determine whether a SAR must be filed.

### International Legal and Regulatory Requests

When the Company receives a legal or regulatory request, such as a subpoena or a judicial order from any jurisdiction (“legal request”), the Company will conduct a risk assessment of the customer subject to the legal request and review the customer’s account activity. If suspicious activity is uncovered during the assessment and review, the Company will evaluate whether a Suspicious Activity Report (SAR) is required and whether the customer should be restricted from future dealings with Axum in accordance with SAR procedures. The Company understands that none of its officers, Covered Persons, or agents may directly or indirectly disclose to the person who is the subject of the legal request its existence, its contents, or the information used to respond to it.

To maintain the confidentiality of any such legal request the Company receives, the process will be as follows:

- Legal requests will generally be received by the Company through its registered agent or designated legal department. The recipient will forward the legal request to the Company Counsel. The Company will work with the Company Counsel to respond appropriately.
- When the Company receives a legal request served on the Company that is or could potentially be related to Anti-Money Laundering (AML) or sanctions compliance, the Company Counsel handling the matter will provide a copy of the request to the Compliance Officer.
- The Resident Compliance Officer will identify all customer accounts that may be associated with the legal requests received by the Company, and each such account will be reviewed for suspicious activity. SARs and other reports will be filed by the Resident Compliance Officer as required, based on the results of this review.

The Compliance Officer, with the assistance of staff or a third-party service provider, will conduct a search of Company records to determine if the subjects of the legal request hold additional accounts or have been parties to transactions.

### Voluntary Information Sharing with Other Financial Institutions

Subject to applicable international laws and regulations, as well as relevant guidance from legal counsel as needed, the Company will share information about individuals suspected of terrorist financing and money laundering with other financial institutions. This collaboration aims to identify and report activities that may involve terrorist acts or money laundering activities and to determine whether to establish or maintain an account or engage in a transaction. In accordance with these international regulations, the Company may be required to file initial notices before any sharing occurs and annual notices afterward, as per the specific requirements of each jurisdiction.

Before the Company shares information with another financial institution, it will take reasonable steps to verify that the other institution is also compliant with the relevant international regulations for information sharing. This may involve obtaining confirmation from the financial institution or consulting a list of compliant institutions if available.

This requirement applies to both affiliated and non-affiliated financial institutions. The Company will obtain the requisite notices from affiliates as needed and follow the required procedures when appropriate.

The Company will employ reasonable procedures both to ensure that relevant information is shared and to protect the security and confidentiality of this information, including segregating it from the Company's other books and records as appropriate.

The Company also will employ reasonable procedures to ensure that confidential information received from another financial institution is not used for purposes other than:

- Identifying and, where appropriate, reporting on money laundering or terrorist activities;
- Determining whether to establish or maintain an account, or to engage in a transaction; or
- Assisting the financial institution in complying with performing such activities.

Investigations Based on Law Enforcement, Regulatory, or Other Requests

Any time the Company receives a request for information from law enforcement, a regulator, or another financial institution regarding a customer of Axum, the Company shall conduct an investigation in accordance with the SAR investigation procedures outlined below to determine if the filing of a SAR is required or otherwise warranted. Such an investigation shall be undertaken regardless of whether the request for information is compulsory or voluntary.

## CHAPTER 4: OFFENCES

### 4.1 Introduction

Curaçao's Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) regime is founded on several key legislative instruments. Both the Company and its employees may be held criminally and administratively liable for breaches of these laws, and failure to comply may result in prosecution, fines, or imprisonment. The main instruments that form the foundation of the AML/CFT framework are the *Penal Code of Curaçao (Wetboek van Strafrecht)*, which contains Articles 430b to 430d addressing money-laundering offences; the *Landsverordening identificatie bij dienstverlening (LID)*, PB 2017 no. 92 concerning customer identification and verification; the *Landsverordening melding ongebruikelijke transacties (LMOT / NORUT)*, PB 2017 no. 99 governing the reporting of unusual transactions and prohibitions on tipping-off; the *Landsverordening op de Kansspelen (LOK)*, which regulates gaming operations and related AML/CFT obligations; and the *Sanctions National Ordinance (N.G. 2014 no. 55)* together with the *Kingdom Sanctions Act (N.G. 2016 no. 54)*, which address targeted financial sanctions.

### 4.2 Money Laundering – Penal Code of Curaçao (Wetboek van Strafrecht)

Articles 430b to 430d of the Penal Code criminalise all forms of money laundering. A person commits money laundering when he or she converts, transfers, conceals, disguises, acquires, possesses, or uses property knowing or having reasonable grounds to suspect that the property represents, in whole or in part, the proceeds of a criminal offence. It is also an offence to assist another person in concealing, converting, transferring, or otherwise dealing with such property so as to disguise its origin or to help the other person to retain or enjoy the proceeds of criminal conduct.

Money laundering may be committed intentionally or through gross negligence. The offence applies to both natural and legal persons and follows an *all-crimes approach*, meaning that any underlying criminal conduct can constitute a predicate offence.

It is a defence for a person to demonstrate that he or she did not know, suspect, or have reasonable grounds to suspect that the property represented the proceeds of criminal conduct. Penalties include imprisonment of up to six years and/or a fine, with increased penalties for habitual or organised activity or where the offence is committed in a professional capacity.

#### 4.3 Customer Due Diligence and Reporting Obligations – LID and LMOT/NORUT

Under the *Landsverordening identificatie bij dienstverlening (LID)*, PB 2017 no. 92, financial institutions, gaming operators, and other designated entities must identify and verify the identity of each customer and beneficial owner prior to establishing a business relationship or executing any transaction that meets the prescribed threshold. Customer due-diligence measures apply to all business relationships and to occasional transactions equal to or exceeding ANG 25,000 (approximately USD 15,000), whether conducted in a single operation or several related operations.

Entities must also identify any person on whose behalf a transaction is being carried out and apply enhanced due diligence where higher risks are present. It is an offence under Articles 5–10 of the LID to fail to perform these identification and verification requirements, to accept false or misleading identification data, or to continue a business relationship without complete due-diligence documentation.

In addition, Article 9 of the *Landsverordening melding ongebruikelijke transacties (LMOT/NORUT)*, PB 2017 no. 99 requires every reporting entity to report unusual transactions to FIU Curaçao without delay, including any attempted transaction that appears to involve the proceeds of criminal conduct, terrorist financing, or an attempt to evade legal obligations. Failure to report, providing incomplete information, or engaging in tipping-off behaviour constitutes an offence subject to fines and/or imprisonment under Articles 14–15 of the LMOT/NORUT.

#### 4.4 Reporting and Tipping-Off – LMOT / NORUT (PB 2017 no. 99)

Articles 9 to 14 of the LMOT require the prompt reporting of unusual transactions to FIU Curaçao. Offences include failing to report an unusual or attempted transaction, providing false or incomplete information, tipping-off by disclosing that a report has been made or that an investigation is underway, and failing to cooperate with FIU Curaçao or obstructing its information requests. Penalties include fines and/or imprisonment as prescribed in Articles 14 to 15 of the LMOT. Curaçao operates an unusual-transaction reporting system, meaning that all transactions meeting FIU indicators must be reported regardless of suspicion.

#### 4.5 Gaming Offences – LOK (Landsverordening op de Kansspelen)

Articles 2 to 7 of the LOK and applicable licence conditions govern the licensing and supervision of gaming activities and embed AML/CFT obligations within licence terms. Offences include operating gaming activities without a valid licence or beyond authorised scope, breaching AML/CFT obligations imposed by the LOK or licence conditions, and failing to maintain internal controls, training, or reporting systems to mitigate AML/CFT risks. Sanctions include administrative fines, suspension or revocation of licences, and where applicable, criminal prosecution.

#### 4.6 Sanctions Compliance – Sanctions National Ordinance and Kingdom Sanctions Act

Articles 3 to 6 of these instruments require entities to comply with targeted financial sanctions related to terrorism and proliferation financing. Offences include failing to freeze the assets of designated persons, making funds or resources available to them, or failing to report a match or suspected match to the competent authority. Penalties consist of fines and/or imprisonment in accordance with Articles 5 to 6 of the Sanctions National Ordinance.

#### 4.7 Destruction or Concealment of Records

Destroying, falsifying, or concealing records relevant to an AML/CFT or sanctions investigation constitutes an offence under Curaçao's Penal Code and related legislation. All records must be preserved for the legally required retention period and made available to FIU Curaçao, the Curaçao Gaming Authority (CGA), or law-enforcement authorities upon request.

### Penalty for failing to report suspicious transactions

A person who contravenes the provisions shall be liable on summary conviction; penalties can range on a scale of up to 20 years imprisonment or an unlimited fine or both.

#### 5. Resident Compliance Officer (RCO) / Money Laundering Reporting Officer (MLRO)

##### 5.1 Resident Compliance Officer (RCO) / Money Laundering Reporting Officer (MLRO)

The Resident Compliance Officer (RCO) / MLRO is the designated employee with overall responsibility for establishing and maintaining effective anti-money laundering and counter-terrorist financing (AML/CFT) systems and controls.

This is a regulatory function that requires prior approval of the individual by the relevant supervisory authority. The regulator expects the RCO / MLRO to be based in Curaçao, possess appropriate seniority and independence, and have unrestricted access to all Know Your Customer (KYC) and Know Your Business (KYB) information held by the Company.

The key responsibilities of the RCO / MLRO include, but are not limited to, the following:

1. Monitoring the effectiveness of the Company's AML/CFT systems and controls.
2. Overseeing compliance with applicable laws, ordinances, and regulatory guidance issued by the Curaçao Gaming Authority (CGA), FIU Curaçao, and other competent authorities.
3. Having overall responsibility for the daily operation and implementation of AML/CFT policies and procedures, even where certain functions are delegated.
4. Ensuring that client acceptance standards remain consistent with Axum's internal policies and regulatory obligations.
5. Receiving, reviewing, and investigating internal suspicious activity disclosures and, where appropriate, submitting external reports to FIU Curaçao in accordance with the *Landsverordening melding ongebruikelijke transacties (LMOT/NORUT)*.
6. Responding promptly to any reasonable request for information from the Curaçao Gaming Authority (CGA), FIU Curaçao, or law enforcement authorities.
7. Acting as the principal liaison between the Company and all external authorities concerning AML/CFT matters.
8. Ensuring that all staff receive appropriate and ongoing AML/CFT training, and that training content and records meet regulatory standards.
9. Reporting to the Board of Directors at least annually through a formal RCO / MLRO Report, and keeping senior management informed of emerging money laundering or terrorist financing risks.
10. Keeping abreast of national and international AML/CFT developments and typologies, including publications and findings of the FATF, IMF, and World Bank.

11. Appointing a Deputy RCO / MLRO to act during temporary absences. Where such absence extends for 12 consecutive weeks or more within a 12-month period, regulatory pre-approval of the deputy is required.
12. Ensuring effective client and transaction monitoring is conducted on an ongoing basis.
13. Conducting continuous assessments of the Company's client base, products, and business activities to identify and mitigate money laundering and terrorist financing risks.
14. Ensuring AML/CFT policies and procedures are communicated clearly and effectively to all relevant employees.

While certain operational duties may be delegated, such delegation must be properly documented. The RCO / MLRO retains ultimate managerial and regulatory accountability for compliance with Curaçao's AML/CFT framework.

## 5.2 Contact with Third Parties

No employee of Axum may discuss the Company's anti-money laundering or counter-terrorist financing policies, procedures, or investigations with any third party without the prior consent of the RCO / MLRO. All requests for information or documentation from regulators, supervisory bodies, or investigative authorities must be immediately referred to the RCO / MLRO for handling.

## 5.3 Orders and Requests from Authorities

The following orders or directions may be served on the Company as part of an ongoing investigation. Any such order received must be forwarded to the RCO / MLRO without delay:

- Production Order
- Disclosure Order
- Client Information Order
- Account Monitoring Order

- Search and Seizure Warrant
- Order for Financial Information under applicable Curaçao legislation

The RCO / MLRO will review and respond to such orders in accordance with the *Landsverordening identificatie bij dienstverlening (LID)*, the *Landsverordening melding ongebruikelijke transacties (LMOT/NORUT)*, and any instructions issued by FIU Curaçao or the relevant judicial authorities.

## CHAPTER 6: THE RISK-BASED APPROACH

### 6.1 Introduction

Axum is required to operate a risk-based policy to identify, manage, and mitigate the risks associated with potential money-laundering or terrorist-financing activity. This approach allows the Company to determine the most effective and proportionate methods of managing exposure to financial-crime risks. A risk-based framework cannot guarantee zero failure; however, it ensures resources are directed toward areas of higher risk, balancing proportionality and practicality. The aim is to focus compliance efforts where they are most needed and will have the greatest impact.

A risk-based approach requires Axum to:

- Assess the risks applicable to its business model and customers. Axum recognises that elevated money-laundering risks arise from the nature of its online operations, where clients are generally accepted on a non-face-to-face basis.
- Enable the Resident Compliance Officer (RCO) / MLRO and the Board to design and implement controls to manage and mitigate these risks.
- Monitor, review, and improve the effectiveness of controls in a cost-efficient manner.
- Reduce risk exposure wherever practicable.
- Document all risk assessments, decisions, and rationale to demonstrate compliance with Curaçao's AML/CFT framework.

### 6.2 Risk Potential

Axum mitigates money-laundering and terrorist-financing risks through several preventive measures, including:

- Robust client-identification standards based on jurisdictional risk.
- No acceptance of cash transactions.
- No acceptance of third-party payments.
- Restrictions on transactions involving higher-risk countries or sanctioned jurisdictions.
- Ensuring, unless otherwise approved by the RCO / MLRO, that all funds are returned only to the originating account from which they were received.

### 6.3 Evaluating the Risk to Axum

The Company adopts a risk-based approach that enables efficient use of resources in proportion to identified risks. While Axum seeks consistent application of this approach, it acknowledges that discretion may occasionally be required. The RCO / MLRO may exercise judgment to deviate from standard policy where warranted, provided such decisions are clearly reasoned and documented.

When assessing risk, Axum considers the following core factors, which are explored throughout this Manual:

#### Non-Face-to-Face Business

Axum conducts its business with individual clients worldwide primarily on a non-face-to-face basis, which inherently increases the risk of impersonation or identity fraud. This risk is mitigated by applying one or more of the following measures:

- Requiring the customer's first payment to originate from a bank account in the customer's own name held with a Curaçao-licensed institution or a financial institution located in a FATF-compliant jurisdiction.
- Requesting supplementary identification or documentation for non-face-to-face clients.
- Verifying contact information through direct telephone communication prior to activation of services.

- Sending account-opening documentation to a verified address and requiring acknowledgment or return.
- Using secure online verification methods, such as tokens or passwords, provided only to verified individuals.
- Requiring document certification by an appropriate certifier (e.g., notary public, attorney, or financial institution officer).

Any subsequent change to the client's name, address, or employment details constitutes a "trigger event" requiring a KYC review. Regular reviews of customer information are integral to Axum's ongoing due-diligence programme.

#### Delivery Channels for Payments

Axum receives funds exclusively through electronic channels. Cash payments are not accepted. Electronic transfers ensure the sender's identity is traceable and can be verified against account-holder information. Any payments received from unconnected third parties are returned to the remitter immediately.

#### Geographic Risk

Axum may engage clients across multiple jurisdictions; however, clients residing in or associated with higher-risk or sanctioned jurisdictions will be subject to enhanced scrutiny. Mitigating factors — such as the client's legitimate business presence in a high-risk country — must be documented and approved by the RCO / MLRO.

#### 6.4 Client Risk Assessment

The Company categorises clients as Low, Neutral, or High risk, based on jurisdiction, customer type, product use, and transactional behaviour. The RCO / MLRO is responsible for determining and recording the risk category and rationale for each client.

Regardless of any exemption or transaction size, customer identity must always be verified where money-laundering or terrorist-financing concerns exist. Where such activity is known or suspected, an internal report must be filed with the RCO / MLRO. If suspicion is confirmed, a disclosure must be made to FIU Curaçao in accordance with the *Landsverordening melding ongebruikelijke transacties (LMOT/NORUT)*. Terrorist-financing concerns should likewise be reported promptly to law-enforcement authorities. Verification procedures must be completed if not already undertaken.

#### 6.5 Risk Assessment for New Products, Services, Practices, or Technologies

Before introducing any new product, service, business practice, or technology, Axum will conduct a documented risk assessment to evaluate its potential to facilitate money-laundering or terrorist-financing activity. This assessment will consider:

- The nature and functionality of the product or service, including potential for anonymity or cross-border use.
- Delivery channels and related exposure, particularly non-face-to-face or digital platforms.
- Geographic risk, especially links to high-risk or sanctioned jurisdictions.
- Technological vulnerabilities that could enable misuse.

Assessment results will be formally documented and retained for supervisory review by the Curaçao Gaming Authority (CGA) or other competent authorities. These evaluations will be periodically revisited to ensure continued relevance as products evolve.

#### 6.6 Additional Measures for High-Risk Scenarios

Where elevated risks are identified, the Company will apply enhanced safeguards, including:

- Enhanced Due Diligence (EDD): Applied to high-risk clients, complex or large transactions, or products that may increase anonymity (e.g., remote digital access).
- Restrictive Measures on High-Risk Products: Limiting or prohibiting services that facilitate anonymous or untraceable activity without sufficient KYC controls.
- Ongoing Transaction Monitoring: Increasing scrutiny of activity linked to high-risk clients, delivery channels, or jurisdictions with inadequate AML/CFT regimes.

## CHAPTER 7: CLIENT DUE DILIGENCE PROCEDURE

## 7.1 Introduction

The Acts set out the firm's obligations to conduct Client Due Diligence ("CDD"). The regulations specify the CDD measures that are required to be carried out, the timing, as well as actions required if CDD measures are not carried out; and, introduce the concept of Simplified Due Diligence (SDD) and Enhanced Due Diligence (EDD).

These procedures are implemented in accordance with the National Ordinance on the Prevention and Combating of Money Laundering and Terrorist Financing (PMLTF) and the AML/CTF Provisions and Guidelines (2022) issued by the CBCS. They apply to all customers, business relationships, and occasional transactions conducted by Axum.

The purpose of this chapter is to provide guidance on the following:

- The meaning of CDD measures;
- Timing of, and non-compliance with CDD measures;
- Application of CDD measures;
- Simplified Due Diligence; and
- Enhanced Due Diligence.

For lists of the documentation to be obtained and verified in respect of specific business types please refer to Chapter 6 of this Manual.

## 7.2 What is CDD?

The CDD measures that must be carried out involve:

- Identifying the Client and verifying the identity;
- Identifying the beneficial owner, where relevant, and verifying their identity;
- Obtaining information on the purpose and intended nature of the relationship;
- Conducting on-going monitoring of the relationship; and

- In the case of legal entities, the firm must understand the ownership and control structure.

These measures are designed to make it harder for the financial services industry to be used to launder money or fund terrorism.

### 7.3 (a) Timing of Verification (Regulation 8(5))

The Company ensures that customer identity is verified in a timely manner, subject to the following procedures:

1. Verification Post-Account Opening:

- In exceptional circumstances, the Company may open an account before completing verification of the customer's identity, provided that:
  - Adequate measures are in place to prevent the account from being operational until verification is completed.
  - This exception is approved by the Resident Compliance Officer(CO) or Resident Compliance Officer(RCO) / MLRO (Resident Compliance Officer(RCO) / MLRO).

2. Controls for Unverified Accounts:

- Accounts opened prior to verification are subject to the following controls:
  - Restricted Transactions: No deposits, withdrawals, or other transactions will be permitted.
  - Temporary Holds: The account remains in a "pending" or "restricted" status until verification is finalized.

3. Escalation Procedures:

- If identity verification cannot be completed within a reasonable timeframe:
  - The account will be flagged for further review.
  - The CO or Resident Compliance Officer(RCO) / MLRO will determine whether to escalate the matter or terminate the relationship.
- 

4. Documentation and Record-Keeping:

- Records of unverified accounts and actions taken to restrict transactions are maintained for regulatory review.
- All instances of accounts opened before verification must be logged, with justification and approval documented.

### 7.3(b) Requirement to Cease Transactions (Regulation 9)

If the Company is unable to apply Customer Due Diligence (CDD) measures, the following actions will be taken to ensure compliance with Regulation 9:

1. Account Opening and Occasional Transactions:
  - The Company will not open an account or carry out any occasional transaction where CDD cannot be completed.
2. Business Relationships and Transactions:
  - The Company will not establish a business relationship or proceed with any occasional transaction if the required CDD measures cannot be applied.
3. Termination of Existing Relationships:
  - The Company will terminate any existing business relationship where it becomes impossible to complete or update CDD measures.
4. Suspicious Activity Reporting (SAR):
  - Where appropriate, the Company will file a Suspicious Activity Report (SAR) with the Financial Intelligence Unit Curaçao (FIU Curaçao) (FIU Curaçao) if the inability to apply CDD raises concerns of money laundering (ML) or terrorist financing (TF)

### 7.4 Application of CDD Measures

The application of CDD measures involves four steps:

- 1) Identifying the client and beneficial owners
- 2) Verifying this information
- 3) Construction of an Economic Profile
- 4) Ongoing monitoring of the relationship

### 7.5 Who is the Client?

The term client is not defined by regulations but, in general, will be the party with whom the business relationship would be established. To this extent, Axum must be satisfied that it is dealing with a real person and for this reason must obtain sufficient evidence of identity to verify that the individual is who they claim to be. In respect of legal corporate entities, the Company must understand the ownership and control structure of the client. Irrespective of the client's type (e.g. sole trader, corporation, trust or partnership) the Company must obtain sufficient data and information regarding the client's business activities and the expected pattern and level of transactions. If in doubt as to who should be identified as the client, please seek guidance from the Resident Compliance Officer(RCO) / MLRO.

### 7.6 Who is the Beneficial Owner?

The regulations require that any natural person who ultimately owns or controls 10% or more of the shares or voting rights in a legal entity or otherwise exercises ultimate effective control over the customer. However, Axum will seek to identify the individuals who have the ultimate control of the business or its assets. In cases where the ultimate control rests with the persons who have the power to manage funds, accounts, or investments of the legal entity, without requiring authorisation, and is in a position to override the internal procedures of the entity.

In light of the inherent risks of opening corporate accounts on a non-face-to-face basis, the Company would seek to identify the corporate structure and those individuals with a direct or indirect interest in excess of 10% of the share capital or voting rights.

### 7.7 Existing Clients

If a client has already been identified and approved by Axum no additional information needs to be obtained in respect of such a client unless the information already available is either out of date, or if the client's risk profile has changed.

### 7.8 Construction of an Economic Profile

Information will be collected during the account opening process before the establishment of a relationship and on an ongoing basis, with the aim of constructing a client's economic risk profile and as a minimum will typically include:

- The purpose and reasoning for the opening of an account;

- The anticipated account turnover;
- The nature of the transactions;
- The expected origins of incoming funds to be credited into the account and any expected destination of outgoing funds;
- Clients' net worth and annual income; and
- An understanding of the main business/professional activities of the client.

## 7.9 Simplified Due Diligence

The Company permits Simplified Due Diligence (SDD) in limited circumstances where the risk of Money Laundering (ML) and Terrorist Financing (TF) is assessed to be low. SDD is applied only after completing a documented risk assessment and ensuring compliance with the following conditions:

### 1. Conditions for Applying SDD:

SDD can only be applied if all the following conditions are met:

- The risk of ML/TF is determined to be low based on a comprehensive risk assessment.
- There is no suspicion of ML/TF associated with the customer, transaction, or account.
- The risk assessment and rationale for applying SDD are fully documented and approved by the Resident Compliance Officer(CO) or Resident Compliance Officer(RCO) / MLRO (Resident Compliance Officer(RCO) / MLRO).

### 2. Permissible Circumstances:

- SDD may be permitted for customers who are:
  - Financial institutions subject to equivalent AML/CTF regulations.
  - Public authorities or state-owned enterprises with transparent structures.
  - Customers in low-risk industries and jurisdictions.
  - Customers who are companies listed on an appointed stock exchange.
  - Employee pension schemes

### 3. Monitoring Requirements:

- Even when SDD is applied, the Company must:
  - Monitor the customer relationship for changes in risk profile and to detect any unusual or suspicious activities.

- Ensure that transactions are consistent with the customer's known profile.
  - Reassess the customer's risk level if new information arises, if the risk profile of the customer changes, if required apply standard or enhanced due diligence measures as appropriate.
4. Documentation:
- The Company must maintain records of:
    - The risk assessment that justifies applying SDD.
    - The specific measures taken and rationale for reduced due diligence.
5. Prohibition in Suspicious Cases:
- SDD will not be applied where there is any suspicion of ML/TF, regardless of the customer's risk level.

### 7.10 Enhanced Due Diligence

Under the risk-based approach adopted by Axum Enhanced Due Diligence (EDD) will need to be conducted on any clients falling into the high-risk category.

In addition to these clients, the regulations state three specific types of relationship where EDD must be applied. These are:

- Where the client is not physically present and does not satisfactorily pass the electronic identification process or adverse or warning information has been gathered during the applicant;
- Any relationship or transaction involving a Politically Exposed Person ("PEP").
- Specific guidance on the application of enhanced due diligence is contained in Chapter 6.

Additional secondary verification including:

- Mail Redirect, confirming mail redirect at address, for anti-fraud reasons.
- Debit & Credit Card Check, confirming card against the residential address, for anti-fraud reasons.
- IP Address Location, confirming IP location cross reference with address, for anti-fraud reasons.

EDD will be required:

1. High-Risk Customers and Transactions: EDD is conducted when customers or transactions present a higher risk of money laundering or terrorist financing. This includes customers involved in high-risk industries, those operating in high-risk jurisdictions, and transactions that are unusually large, complex, or inconsistent with normal business activities.
2. Politically Exposed Persons (PEPs): Customers who are PEPs or have close associations with PEPs pose a greater risk due to their potential exposure to corruption. EDD is necessary to ensure a thorough understanding of the source of their wealth and the legitimacy of their financial activities.
3. Unusual or Suspicious Activity: When unusual patterns or suspicious activities are detected, EDD is performed to gather additional information and assess the underlying purpose and legitimacy of the customer's transactions.
4. Complex Ownership Structures: EDD is necessary for customers with complex or opaque ownership structures that may obscure the true beneficial owner(s). This ensures transparency and reduces the risk of being unknowingly involved in illicit activities.
5. Adverse Media or Negative Information: Customers or entities that have been subject to negative media coverage or have known associations with criminal activities require EDD to evaluate the potential reputational and financial risks to our organization.
6. Regulatory and Legal Obligations: In some cases, EDD is a regulatory requirement, particularly when dealing with high-risk categories as defined by local and international AML regulations. Conducting EDD ensures compliance with these legal obligations and helps safeguard the organization against regulatory penalties.

### 7.11 Exception to Full Identification

While we will use our standard account opening procedure to verify the identity of our clients whenever possible; it may be the case that a client cannot provide standard information, or there are other factors that may influence the client's risk-profile. Axum procedures cannot accommodate every eventuality and, in some cases, the Resident Compliance Officer(RCO) / MLRO will need to exercise their judgement. This may justify a deviation

from the firm's standard client opening procedure. All such exceptions must be agreed and documented by the Resident Compliance Officer(RCO) / MLRO in accordance with the Company's risk-based approach.

## 7.12 Standard of Verification Evidence

### Client Risk

The level of documentation required for each client will vary depending on the risk category of a particular client.

### Financial Services Targets

It is a criminal offence to make funds or financial services available to sanctioned entities and people (targets) on the Financial Sanctions list. This would include dealing directly with these targets and dealing with these targets through intermediaries (such as lawyers or accountants).

Please reference the attached Appendix for a Consolidated List of Financial Sanctions Targets.

### Origin of Documents

Generally, when identifying a client, a document issued by a government department or agency, or by a court will provide a high level of confidence. The Company will normally accept non-government issued documentary evidence verifying identity only if it originates from a public-sector body or a regulated financial services firm in an equivalent jurisdiction

### Documents in a Foreign Language

If documents are in a foreign language, the Firm will take appropriate steps to be reasonably satisfied that the documents do in fact provide evidence of the client's identity. This is likely to involve translation of either all or part of a document, by a designated Firm's employee with the appropriate skills to undertake the language translation required or an external approved third party. Under no circumstances will Axum seek to place reliance on any translated documents provided by a client or applicant.

## Documentary and Electronic Identification and Verification

Axum may rely on either documentary, electronic, or a combination of documentary and electronic identification evidence. The Company will seek to facilitate electronic evidence where suitable, and data will be verified using multiple sources, and will incorporate qualitative checks that assess the strength of the information supplied and if no reasonable verification can be obtained electronically, the Company will apply the standard documentary verification requirements.

Axum cannot rely exclusively on electronic systems that access data from a single source only (e.g. a single check against the Electoral Roll).

## Electronic Identification and Verification Providers

Electronic identification and verification is undertaken by Axum under a contract with an approved third-party supplier. In accordance with the regulations, a supplier must meet the following criteria:

- it is recognised, through registration with the Information Commissioner's Office to store personal data;
- it uses a range of positive information sources that can be verified to link a potential client to both current and previous circumstances;
- it is able to access sources of information to collect negative information sources, such as data bases relating to fraud or deceased persons;
- it accesses a wide range of alert data sources; and
- It has transparent processes that enable the Company to know and understand what data sources have been used, the results of data search, and the value of certainty the source has verified the data provided by the potential client.

For further information on the use of electronic evidence please consult the Resident Compliance Officer or Resident Compliance Officer(RCO) / MLRO.

## Certification of Documents

Where possible, we will seek to obtain certified copies of identification documents. Some clients may reside out of Curaçao and not have machine-readable documents, such as a passport. In these cases, each document needs to contain a statement that the document is a certified copy of the original and must be dated and signed by one of the following. A non-exhaustive list is detailed below:

- Solicitor or notary public;
- Banker;
- Auditor or Accountant;
- Consulate or government official;
- A Axum' designated employee who has seen the original document;
- In addition, a person who certifies a document should provide their contact details.

#### Client's Websites

The Company understands that although the information on the websites of its clients or potential clients may be helpful, it is not independently verified. While Axum may use such information as corroborative evidence, it will not exclusively rely on it without an exception granted by the Resident Compliance Officer(RCO) / MLRO for low-risk clients.

#### Public Information

Listed and some unlisted public companies are subject to a high level of disclosure in relation to ownership and business activities; and may have public filing obligations. Private companies and some partnerships, although not subject to such a level of disclosure, often have public filing obligations. Whenever possible and appropriate, the Firm will seek to use reliable public information in its identification process.

#### Signatories

On some occasions, and where appropriate, Axum may be provided with a list of those authorised to give instructions for the movement of funds or assets, along with an appropriate instrument authorising one or more directors (or equivalent) to give the Company such instructions. Axum will use this information in determining whom to identify, using its risk-based approach.

### Non-Face-to-Face Clients

Taking into consideration Axum's business model, it is highly likely the Company would not meet our clients face to face either during the application process or following approval.

As the Company's clients will be predominantly accepted without face-to-face contact, non-face-to-face business will not in itself increase Axum a money laundering risk posed by a particular client. However, non-face-to-face identification carries an inherent risk of impersonation fraud. To mitigate this risk the Firm will perform additional processes, such as:

- The use of software providers to check the authenticity of passports provided by potential clients during the application process;
- The use of an electronic identification provider to verify the identity of an applicant using various data sources;
- Telephone contact may be conducted with the client using contact details provided during the application process;
- Requiring copy documents to be certified or notarized by an appropriate person, if they are required; and Enhance Due Diligence to be performed
- Digital or physical email or mail letters may be sent requiring further verification from the client where applicable and reasonable (and any returned mail or bounced email will be investigated and documented with additional measures taken); and
- The invite-only closed ecosystem nature of our marketing growth model; every new client is known directly by at least one other client.

### Controller of Funds

If it appears that another person may have control over the funds which form or otherwise relate to the relationship with our client, we will seek to identify the controller as well as the client, if and when justified by risk.

### Other Considerations

Passport copies should be in colour (not black and white), wherever possible. Clients should be discouraged from sending original valuable documents by post.

Consideration should be given as to whether the documents relied upon may have been forged.

### 7.13 Prohibited Business Activities

The following business activities are strictly prohibited due to their inherent risks, legal implications, and potential for involvement in illegal activities such as money laundering, terrorist financing, and other forms of financial crime. Engaging in these activities may expose the organization to significant regulatory, legal, and reputational risks:

1. Shell Banks and Shell Companies:

The organization will not establish or maintain business relationships with shell banks or shell companies, which are entities without a physical presence or significant business operations. These entities are often used to obscure the identity of the beneficial owners and facilitate illegal activities.

2. Prohibition of Anonymous and Fictitious Accounts:

The Company will not set up anonymous accounts, anonymous passbooks, or accounts under obviously fictitious names for any new or existing customer. All accounts must be linked to verified, identifiable individuals or entities in accordance with our Client Due Diligence (CDD) procedures.

3. Unlicensed Money Service Businesses (MSBs):

The organization will not engage with unlicensed or unregulated money service businesses, including those involved in money transmission, currency exchange, or payment processing without the appropriate regulatory approvals.

4. Businesses Operating in High-Risk Jurisdictions:

The organization will avoid conducting business with entities located in or operating from jurisdictions identified as high-risk for money laundering, terrorist financing, or other financial crimes by international bodies such as the Financial Action Task Force (FATF).

5. Illegal Gambling Operations:

The organization will not engage with or provide services to illegal gambling operations, including online gambling platforms that do not hold the necessary licenses or operate in jurisdictions where gambling is prohibited.

6. Unregulated Virtual Asset Service Providers (VASPs):

The organization will not conduct business with virtual asset service providers (e.g., cryptocurrency exchanges or wallet providers) that are unregulated or fail to comply with applicable anti-money laundering (AML) and counter-terrorism financing (CTF) regulations.

7. Businesses Involved in Human Trafficking or Exploitation:

The organization will not engage with entities that are involved in human trafficking, exploitation, or other forms of modern slavery, as these activities are illegal and carry severe criminal penalties.

8. Production and Distribution of Counterfeit Goods:

The organization will not engage with businesses involved in the production, distribution, or sale of counterfeit goods, including counterfeit pharmaceuticals, luxury goods, or technology products.

9. Unlicensed Firearms and Weapons Dealers:

The organization will not establish or maintain relationships with businesses involved in the illegal trade of firearms, weapons, or related materials without the proper licenses and regulatory approvals.

10. Environmental Crimes:

The organization will not support or conduct business with entities involved in illegal activities that harm the environment, such as illegal logging, poaching, or unregulated mining operations.

## 11. Pornography and Adult Entertainment:

The organization will not engage in business relationships with entities involved in the production, distribution, or promotion of illegal or unregulated pornography and adult entertainment, particularly where such activities exploit minors or involve non-consensual acts.

### 7.14 Ongoing Monitoring

The Company will continuously monitor the business relationship to ensure transactions are consistent with the customer's known risk profile, business activities, and source of funds. Ongoing monitoring includes:

- Reviewing customer information and documentation to keep it up to date;
- Identifying changes in ownership, control, or business activities; and
- Scrutinising transactions to ensure they are consistent with the purpose and intended nature of the relationship.  
Any material inconsistencies identified must be escalated to the Resident Compliance Officer (RCO) / MLRO.

## CHAPTER 8: IDENTIFICATION EVIDENCE AND KYC

### 8.1 Introduction

Customer Due Diligence ("CDD") is Axum's primary defence against being unwittingly used for money laundering, terrorist financing, or other criminal activity. CDD is an integral part of Axum's AML/CTF Program and is implemented in accordance with the National Ordinance on the Prevention and Combating of Money Laundering and Terrorist Financing (PMLTF), the AML/CTF Provisions and Guidelines of the Central Bank of Curaçao and Sint Maarten (CBCS), and related local requirements.

Axum must establish and maintain relationships only with customers whose identity is known and verified, and whose source of wealth, source of funds, and business activities are believed to be legitimate. All client-facing employees must exercise sound judgement when accepting new customers and reviewing existing ones and must escalate concerns to their supervisor and/or the Resident Compliance Officer (RCO) / MLRO.

CDD begins at onboarding and continues throughout the life of the relationship. Appropriate Know Your Customer (KYC) information must be obtained at onboarding and reviewed on a risk-based and periodic basis thereafter. Robust CDD policies, procedures, and processes—especially for higher-risk customers—enable Axum to identify and report unusual or suspicious activity.

KYC verification scope. Identification must be obtained for all relevant natural persons (account holders, beneficial owners, authorised signatories, attorneys-in-fact, controllers) and for all legal entities and structures. If a prospective customer does not fit the categories below, seek guidance from the RCO/MLRO.

## 8.2 Customers Eligible for Simplified Due Diligence (SDD)

Axum may apply SDD only where a documented risk assessment supports a low ML/TF risk and there is no suspicion of ML/TF. SDD does not remove the obligation to identify the customer; it allows reduced verification measures commensurate with risk.

Categories (examples):

- Regulated financial institutions in Curaçao, the UK/EU, FATF members, or Equivalent jurisdictions.  
Obtain and retain:
  - Evidence of regulatory/supervisory status (e.g., licence, register extract).
  - Registered/business address evidence.
- Public authorities and community institutions (Curaçao/UK or equivalent).  
Obtain and retain:
  - Evidence of public status and legal existence.
  - Address evidence.
- Listed companies on a regulated or equivalent market (including ≥50% consolidated subsidiaries).  
Obtain and retain:

- Proof of listing (or subsidiary status) and address evidence.

Where the market is outside the EEA, Axum records the steps taken to confirm the market's disclosure regime is equivalent.

Note: If risk indicators emerge, revert to standard or enhanced due diligence.

Companies subject to statutory licensing/prudential regimes (e.g., OFWAT, OFGEM, OFCOM, or EU equivalents) may be considered for SDD, subject to the above principles.

### 8.3 Customers Subject to Full Identification Requirements

- Natural Persons
- Unregulated Private Companies
- Partnerships and Unincorporated Businesses
- Limited Partnerships
- Non-Government/Public Authorities outside Curaçao (tailored approach)
- Trusts, Foundations, and similar entities
- Unregulated Funds

Axum always obtains Standard Information and layers on additional verification based on the customer's risk rating (see Chapter 4).

### 8.4 Natural Persons

Axum verifies, at a minimum:

- Full name

- Residential address
- Date and place of birth

Acceptable verification (one of):

A) One government-issued document with photo showing full name and (address or date of birth); or

B) One government-issued document (no photo) with full name plus a second document (government/judicial/public-sector/regulated firm) showing full name and (address or date of birth).

Electronic identification mirroring the above (multiple independent data sources) may be used. For non-face-to-face onboarding, Axum reviews originals or certified/notarised copies where feasible.

Axum screens individuals (customers, beneficial owners, directors/officers) for:

- Sanctions
- Politically Exposed Persons (PEP)
- Adverse media

Potential matches are escalated to the RCO/MLRO for decision.

High-Risk Individuals — EDD (additional to the above):

1. Identity: Current passport or national ID (photo page and relevant details).
2. Address: At least one original document (by preference):
  - National ID (if not used for identity)
  - Photo driving licence

- Government correspondence (≤12 months)
- Social security card (showing address)
- Council tax demand/statement (≤12 months)
- Bank/credit card statement (≤3 months)
- Mortgage statement (≤3 months)
- Utility bill (not online printouts)  
If at current address <6 months, evidence of previous address is required. No c/o or P.O. Box as residential address.

3. Source of funds (SoF): e.g., bank statement of remitting account in customer's name; further SoF/SOW as warranted.

## 8.5 Unregulated Private Companies

### Standard Information (examples):

1. Official document with full legal name and registration number
  - e.g., Certificate of Incorporation / Partnership Agreement
2. Registered office address (jurisdiction of incorporation)
3. Business/trading address (e.g., utility bill, government doc, site visit record)
4. Names of all directors
5. Names of all direct and indirect beneficial owners holding ≥10% of shares/votes (if none at ≥10%, the RCO/MLRO designates controlling persons to verify on a risk basis)

6. Latest audited financial statements (where available)
7. Group/shareholding chart (where relevant)

Where possible, obtain information from independent sources (official registers, reputable data providers). Verify:

- At least one director and all BOs at  $\geq 10\%$  as natural persons (see 8.4).

EDD for High-Risk Companies (in addition):

- Identification of all executive directors and controllers per individual requirements.
- For PEP involvement: Senior Management Approval (SMA) and robust SoF/SOW; apply heightened monitoring.

#### 8.6 Partnerships & Unincorporated Businesses

Treat per private companies, with adjustments:

Standard Information:

1. Trading address
2. Nature of business
3. List of all partners
4. Partnership deed (if any)
5. Latest financial statements (audited where available)

Verify partners/beneficial owners with  $\geq 10\%$  interest as individuals. If a partner is a legal person, identify and verify its ultimate beneficial owner(s)  $\geq 10\%$ .

### 8.7 Limited Partnerships

Treat as private companies, with a list of partners in place of directors/BOs. Verify partners/beneficial owners  $\geq 10\%$ , including the General/Managing Partner as a natural person. If the GP/MP is a company, verify its ultimate BO(s).

### 8.8 Non-Government & Public Authorities (outside Curaçao)

Apply a tailored approach; obtain at minimum:

1. Full legal name
2. Nature/status of entity
3. Address
4. Home-state authority
5. Names of governing officials (or equivalents)

Verify name, address, and—where appropriate—home-state authority. For high-risk authorities, verify directors/controllers as individuals.

#### Unregulated Funds (additional guidance)

- Reputable Service Providers: Consider the presence of regulated administrators, prime brokers, custodians when risk-rating the fund.
- Transparency of Ownership: Understand and document multi-layer structures; focus on ultimate controllers (e.g., IM, adviser, board).

- Feeder/Master: Verify at least the Feeder Fund. For investors >10%, either:
  - A) Verify directly; or
  - B) Obtain written assurance from a responsible (preferably regulated/equivalent) party that
    - such investors have been KYC'd appropriately; or
    - their identities will be disclosed for Axum verification; or
    - there are no >10% investors.Document and periodically re-confirm such assurances.
- Start-Up Funds: Monitor during pre-investor phase and perform investor KYC once holdings >10% are reasonably established.

#### 8.9 Politically Exposed Persons (PEPs)

Axum screens all individual customers, directors/officers of entity customers, and ultimate beneficial owners ≥10% for PEP status at onboarding and on an ongoing basis.

Definition (summary): Individuals who hold or have held prominent public functions—foreign, domestic, or international organisation PEPs—including family members and close associates.

EDD requirements for PEP relationships:

- RCO/MLRO investigation of any potential match and Senior Management Approval prior to onboarding.
- Obtain/assess Source of Wealth (SOW) and Source of Funds (SoF).
- Heightened monitoring, with at least annual formal review by the RCO/MLRO.
- Consider jurisdiction risk, role/influence, adverse media, and any sanctions links.

#### 8.10 Missing / Incomplete CDD

CDD should be completed before account opening. In exceptional cases approved by the RCO/MLRO, the account may be opened with strict controls (e.g., restricted/non-operational status).

- Completion Deadline: CDD must be completed within 30 working days of exceptional approval.
- If incomplete at 30 working days: place/maintain full restrictions (no transactions other than returning incoming funds to origin).
- If incomplete at 90 working days: terminate the relationship and return funds to the original source, unless otherwise directed by the RCO/MLRO.
- Cross-border transfers are prohibited until the account is fully compliant.
- If the customer refuses or discussions break down, submit an Unusual Activity Report (UAR) to the RCO/MLRO, who will determine whether to file an Unusual Transaction Report (UTR) with FIU Curaçao.

#### 8.11 Ongoing Monitoring & Periodic Refresh

Axum conducts risk-based ongoing monitoring to ensure activity aligns with the customer's profile, purpose, and SoF/SOW.

Minimum periodic KYC refresh cycles (unless a trigger occurs earlier):

- High risk: Annually
- Medium risk: Every 2–3 years
- Low risk: Every 3–5 years

Trigger events (refresh/update as needed): changes in ownership/control, PEP status, adverse media, sanctions, atypical activity, product/geographic changes, or internal risk re-rating.

#### 8.12 Documentary & Electronic Verification Standards

- Prefer government-issued/official documents; use independent sources where possible.
- Electronic verification must use multiple data sources and provide transparency of data provenance and match strength.
- Axum will not rely solely on a single-source electronic check (e.g., Electoral Roll only).
- Documents in foreign languages must be translated by a qualified Axum employee or an approved third party—not by the customer.

Certification: Certified copies should state they are a “true copy of the original,” include the certifier’s name, title/firm, signature, date, and contact details. Acceptable certifiers include solicitors/notaries, bankers, auditors/accountants, consular/government officials, or an authorised Axum employee who has seen the original.

Non-face-to-face mitigants: document authentication tools, electronic ID, call-backs, certified copies, bounce-mail checks, and (where appropriate) EDD.

#### 8.13 Signatories & Controllers of Funds

Obtain and, where appropriate, verify the identities of those authorised to give instructions and those with control over funds related to the relationship (even if not the customer), commensurate with risk.

#### 8.14 Prohibited Business Activities

Axum does not onboard or maintain relationships involving: shell banks/companies; anonymous/fictitious accounts; unlicensed MSBs; high-risk jurisdictions absent adequate mitigation; illegal gambling; unregulated VASPs; human trafficking/exploitation; counterfeit goods; unlicensed weapons; environmental crimes; and illegal/unregulated pornography or adult entertainment, particularly where minors or non-consensual acts are involved.

### 8.15 Reliance & Outsourcing

Where Axum relies on a third party to perform aspects of CDD, Axum remains ultimately responsible. Reliance is permitted only where the third party is regulated in an Equivalent jurisdiction, Axum obtains immediately the necessary CDD data/copies on request, and a written agreement is in place. Outsourced providers must meet Axum's standards and be subject to oversight.

### 8.16 Record-Keeping & Data Protection

Axum retains CDD records, transaction records, screening logs, and monitoring outcomes for at least five (5) years after the end of the relationship (or longer if legally required). Personal data is processed in accordance with applicable data protection laws and Axum's Privacy Policy.

### 8.17 Practical Notes

- Passport copies should be colour where possible. Customers should not mail original valuable documents.
- Consider the risk of forgeries; use appropriate document-checking tools.
- Customer websites may be used as corroborative evidence only—never as the sole source—unless expressly permitted by the RCO/MLRO for low-risk cases.

## CHAPTER 9: OUTSOURCING

### 9.1 Regulatory Requirement

Subject to approval of the CGA, Axum may operate:

- Exchange;
- Crypto wallet; and

- Custodial wallet services.

Axum must inform the CGA prior to entering any outsourcing arrangement for material services (e.g., technology operations, custody operations, KYC/AML operations, transaction monitoring, incident response, data hosting). The Chief Executive Officer (or delegated Senior Manager) approves all outsourcing arrangements in line with this policy.

Axum will notify the CGA without undue delay of any adverse development in an outsourcing arrangement that may significantly impact the Company or customers, including prolonged service failure/disruption or any security/confidentiality breach affecting Company or customer data.

Scope. This Chapter applies to all third-party and intra-group outsourcing arrangements supporting Axum's regulated activities, including cloud and managed service providers.

## 9.2 Materiality

An arrangement is Material if a failure or security breach could materially impact:

- Business operations, reputation, or profitability; or
- Axum's ability to manage risk and comply with laws/regulations; or
- Customers (e.g., unauthorised access/disclosure/loss/theft of customer information).

Factors considered when assessing materiality include:

- Importance of the outsourced activity (contribution to revenue/critical service delivery);
- Potential impact on earnings, solvency, liquidity, funding, capital, risk profile;
- Reputational/brand impact and ability to meet business objectives if the provider fails;
- Customer harm (service unavailability; data compromise);

- Outsourcing cost as a proportion of total operating cost;
- Cost and feasibility of replacing the provider, and time to restore service.

Presumption of materiality: Outsourcing of risk management and control functions (compliance, internal audit, financial accounting), core platform operations, custody, KYC/AML/transaction monitoring, security operations, or core cloud infrastructure is considered Material.

### 9.3 Evaluation of Outsourcing Risk

The Board and Senior Management oversee outsourcing risk within Axum's risk appetite. Before onboarding or renewing a provider, Axum conducts a documented risk assessment that considers:

#### Axum perspective

- Whether the arrangement provides capability/resources Axum lacks, and is cost-effective;
- Whether Axum retains sufficient in-house expertise to oversee the provider;
- Potential for service disruption to trigger confidentiality/integrity/availability (CIA) breaches;
- Concentration risk (over-reliance on a single provider/region/market).

#### Service provider perspective

- Track record, business reputation, financial strength and going-concern risk;
- Governance, compliance culture, and ethical standards;
- Physical and IT security controls at least equivalent to those of a regulated entity;
- Regulatory standing/licensing (where relevant) and willingness to provide regulatory access;

- Incident response maturity, BCP/DR capabilities (including RTO/RPO), and test evidence.

Independent references/market feedback and onsite or virtual assessments should be obtained where proportionate.

#### 9.4 Governance, Roles & Responsibilities

- Board: Approves outsourcing policy, sets risk appetite, reviews outsourcing register and material arrangements at least annually.
- CEO / Senior Management: Approves individual material arrangements, ensures resources for oversight, and reports incidents to CGA.
- RCO/MLRO & Compliance: Reviews regulatory implications, ensures ongoing compliance (e.g., data protection, AML where relevant), monitors conduct/controls, and reviews contract clauses.
- Information Security (CISO or delegate): Assesses security architecture, data flows, access controls, encryption, logging, and cloud posture.
- Business Owner: Owns the relationship, KPIs/SLAs, risk assessment, and exit plan.
- Internal Audit: Provides independent assurance over third-party risk management.

#### 9.5 Due Diligence (Pre-Contract)

For all providers (depth is risk-based; enhanced for Material):

- Corporate profile, ownership, financials, insurance coverage;
- Certifications/assurance: ISO 27001/27701, SOC 2 (Type II), PCI DSS (if applicable), penetration test summaries, vulnerability management practices;
- Data protection & privacy: data categories processed, retention, deletion/return guarantees, cross-border transfers, subcontractor list;
- Security: network segmentation, encryption at rest/in transit, key management, identity and access management (IAM), privileged access, logging/SIEM, vulnerability scanning/patching cadence, secure SDLC;

- Operational resilience: BCP/DR, last test results, RTO/RPO commitments, capacity and availability design (e.g., multi-AZ/region for cloud);
- Compliance: AML/KYC competence if performing regulated support, sanctions screening controls (where relevant);
- Incident response: timelines, customer notification processes, regulator notification readiness;
- Right to audit/access: acceptance of Axum/ auditor/ regulator access.

Document the DD outcome, risk rating, and mitigating controls before contract signature.

#### 9.6 Contracting Standards (Minimum Clauses)

All outsourcing contracts (and Statements of Work) must, proportionate to risk, include:

1. Scope & services; measurable SLAs/KPIs; service credits and remedies.
2. Compliance with law/regulator rules; provider to support CGA oversight.
3. Data handling: categories, purposes, data minimisation, retention, deletion/return on exit; format and cost for data export.
4. Security controls: baseline standards, encryption, IAM, logging, vulnerability management, change management, secure development, segregation of duties, location of data.
5. Incident management & notification: immediate to Axum, and Axum's right to notify customers/CGA; defined max notification times (e.g., initial notice within 24 hours of detection for material incidents).
6. Right to audit and regulatory access (including CGA and other competent authorities), plus cooperation with supervisory reviews.
7. Subcontracting: prior written approval for Material services; full list of subcontractors; provider remains fully liable.
8. Business continuity/DR: tested plans, RTO/RPO, evidence of periodic tests, participation in Axum-led tests.

9. Performance reporting: regular MI (SLAs, security posture, incidents, capacity metrics).
10. Termination & exit: orderly transition, step-in rights for critical services, continued assistance, data return/deletion certificates, and IP/licence provisions to maintain continuity.
11. Change control: approval for material changes (e.g., hosting region, security model, key subcontractors).
12. Confidentiality & IP; restrictions on use of data for training models unless expressly permitted.
13. Liability & indemnities aligned to risk (including data/security breaches).
14. Law & jurisdiction suitable for enforcement and regulator access.

#### 9.7 Oversight & Monitoring (Post-Contract)

- Service monitoring: Track SLAs/KPIs, capacity, backlog, change failures, incident counts/MTTR, and compliance attestations.
- Control monitoring: Periodic reviews of security posture (e.g., SOC 2 reports, ISO certificates, pen test summaries), evidence of remediation of findings.
- Risk re-assessment: Annual (minimum) for material providers or upon trigger events (major change, incident, M&A, financial distress).
- Senior reporting: Quarterly summary of material providers to Senior Management; annual review by the Board.

#### 9.8 Cloud & Information Security Requirements

For cloud or hosted services:

- Architecture: multi-AZ/region resilience where proportionate; documented data residency.
- Encryption: data at rest and in transit; managed keys or Axum-controlled KMS for sensitive data where feasible.

- Access: least privilege, MFA for admins, JIT/PAM for privileged tasks, quarterly access recertification.
- Logging & detection: centralised logs, immutable storage, retention aligned to law, active monitoring/alerting.
- Secure SDLC: code scanning, dependency management, change approval, segregation of environments.
- Data classification & minimisation: only necessary data processed; pseudonymisation/anonymisation where possible.
- Third-party AI/ML: no customer personal data used to train external models unless contractually permitted, assessed, and disclosed.

#### 9.9 Subcontracting / Fourth Parties

Providers must obtain Axum's prior written approval before appointing subcontractors for Material services and maintain an up-to-date list. Providers remain fully responsible for subcontractor performance and compliance with this Chapter. Axum may perform targeted due diligence on key subcontractors.

#### 9.10 Location & Cross-Border Risk

Axum documents where services and data are processed/stored and evaluates:

- Jurisdictional legal/regulatory constraints, data access by foreign authorities;
- Sanctions, geopolitical risk, disaster/catastrophe exposure;
- Availability of skilled support and time-zone coverage.

Relocation of data/services requires change control and, where material, CGA notification.

#### 9.11 Business Continuity, Exit & Step-In

Each material arrangement must have an Exit/Transition Plan and BCP/DR arrangements including:

- Defined RTO/RPO consistent with Axum's impact tolerances;
- Tested failover/recovery at least annually (evidence retained);
- Data escrow/replication or export formats to enable migration;
- Step-in rights (or equivalent measures) allowing Axum to assume control or appoint an alternative in emergencies to safeguard customers and compliance.

#### 9.12 Incident Management & CGA Notification

Providers must notify Axum of any incident affecting service availability, data confidentiality/integrity, or regulatory compliance immediately on detection, with:

- Initial report within 24 hours (material incidents), including scope, impact, containment steps, and customer/regulatory implications;
- Root cause analysis and remediation plan within agreed timelines;
- Ongoing updates until closure.

Axum will notify the CGA without undue delay where incidents may significantly impact customers or regulated services.

#### 9.13 Records, Registers & Periodic Review

- Maintain an Outsourcing Register covering scope, materiality, data processed, location(s), subcontractors, due diligence date, risk rating, contract dates, SLAs, BCP/DR, and exit status.
- Keep due diligence, assessments, contracts, assurance reports, and monitoring evidence for at least five (5) years after termination (or longer if required).
- Conduct annual policy effectiveness review; update upon regulatory change or material findings.

#### 9.14 Intra-Group Outsourcing

Intra-group arrangements are not automatically lower risk. Axum applies the same risk assessment, due diligence (tailored), contracting (or binding service schedules/policies), monitoring, and regulatory access requirements to group entities, with clearly defined responsibilities and SLAs.

#### 9.15 Prohibited Practices

- Outsourcing that prevents CGA access to data, systems, premises, or staff relevant to Axum’s regulated activities;
- Arrangements that impede Axum’s ability to meet legal/regulatory obligations;
- “Black-box” services without transparency into controls for Material functions.

#### 9.16 Roles Interface with Other Policies

This Chapter must be read with: Information Security Policy, Data Protection/Privacy Policy, Incident Response Procedure, BCP/DR Policy, and Vendor Management SOPs.

#### 10.1 Internal Reporting (to RCO/MLRO)

Obligation to report. Every employee must submit an internal Unusual/Suspicious Transaction report to the Resident Compliance Officer (RCO) / MLRO immediately upon knowing, suspecting, or having reasonable grounds to suspect ML/TF—irrespective of whether Axum ultimately onboards or serves the person. Making an internal report does not breach confidentiality or data-protection obligations.

How to report.

1. Use the prescribed Internal UTR Form (Appendix 1) and submit immediately with all known details.

2. The RCO/MLRO will assess the report in context (KYC file, profile, transaction history, screening, external data).
3. The RCO/MLRO has unrestricted access to internal information needed for assessment and may request further details from the business owner.

Objective test. A failure-to-report offence may arise where an employee ought reasonably to have suspected ML/TF in the circumstances. Staff must know the customer, business rationale, and facts, and make reasonable enquiries consistent with their role.

Timing. Reports to the RCO/MLRO must be made as soon as reasonably practicable after suspicion arises.

Discharge of responsibility. Submitting the internal report discharges the employee's duty under Curaçao's AML framework (e.g., NORUT/NOIS/PMLTF). The RCO/MLRO will issue a written acknowledgement—retain it.

Consultation / duplicate reporting. Employees may seek advice from their line manager, but managers cannot block a report. To avoid duplicates, a consulted colleague should only file separately if they reasonably believe the report will not be made. Limit discussion to need-to-know to avoid tipping-off.

Continuous obligation. Subsequent suspicions (same or different customer) require fresh internal reports.

Post-report activity. Any further transactions or activity related to the subject must be reported to the RCO/MLRO at once.

## 10.2 External Reporting to FIU Curaçao (UTR)

If the RCO/MLRO knows, suspects, or has reasonable grounds to suspect ML/TF or an unusual transaction per NORUT indicators, they will file an Unusual Transaction Report (UTR) to FIU Curaçao via goAML without undue delay, including intended transactions that meet indicators.

- Portal & registration: Axum is registered with FIU Curaçao and reports via goAML.
- Indicators: Sector-specific and generic indicators (objective/threshold and subjective) published by FIU Curaçao guide whether a transaction is unusual and must be reported.
- No "consent clock." Curaçao's regime is not the UK POCA "DAML/7-day consent" model; do not wait for consent unless FIU/law-enforcement expressly instructs you. Remove references to "7 working days" and "consent SARs."

The RCO/MLRO documents the decision to file or not file and the rationale (with supporting evidence). Delays in reporting are a known supervisory concern—timeliness matters.

### 10.3 Monitoring, Red Flags & Case Handling

Axum monitors fiat and digital-asset activity to identify red flags and patterns. The Company may use blockchain analytics to assess wallet risk and linkages to known bad actors. A red flag triggers enhanced scrutiny; it does not automatically equal suspicion.

- The RCO/MLRO (or designee) oversees alert review, escalation, and decisions.
- If no UTR is filed, the RCO/MLRO records the investigation and the reasoned basis for the decision.

Illustrative red flags (not exhaustive): transactions lacking economic rationale; refusal to provide KYC/SoF; short-lived or reactivated dormant accounts; complex/offshore structures with no business logic; unnecessary third-party fund routing. (See Appendix 4: Sample Red Flags.)

### 10.4 Investigation & Escalation Steps

When a red flag is detected:

1. Notify RCO/MLRO immediately.
2. Open a case (RCO/MLRO) and capture: parties, wallets/accounts, amounts, chronology, links, jurisdictions, SoF/SOW, internal notes, and documentary evidence.
3. Widen the lens: review linked/referring customers in Axum's social graph and any common wallets/beneficiaries.
4. Interim risk controls (as appropriate): holds, limits, or suspension pending review.
5. Decision: file UTR via goAML (include a clear narrative) or document "no-UTR" decision with rationale.

6. Law-enforcement engagement: For urgent matters (e.g., TF or ongoing ML schemes), the RCO/MLRO (with counsel) may contact authorities promptly in addition to filing the UTR.

Narrative quality. Draft UTR narratives so an external reader unfamiliar with Axum or virtual assets can follow the facts: who/what/when/where/why/how, parties and roles, dates, values, wallets/accounts, jurisdictions, and flow of funds (source, path, destination). Reference applicable FIU indicators.

Confidentiality. UTRs and related case information are confidential. Staff must not disclose a UTR or its existence externally (including to the customer). All third-party requests (police, customs, regulators) are routed to the RCO/MLRO.

Records. Maintain case files (UTR copy/acknowledgement, investigation notes, evidence, decisions) in secure repositories with restricted access.

#### 10.5 Pre- and Post-Transaction Handling (Tipping-off Control)

- If a transaction is under review (potential UTR), employees must liaise with the RCO/MLRO before engaging the customer. Provide neutral responses about operational checks; avoid tipping-off.
- If FIU/law-enforcement instructs to delay, monitor, or proceed, follow that instruction and record it.
- After a UTR filing, unless directed otherwise by FIU/law-enforcement, activity may resume subject to risk controls determined by the RCO/MLRO.

#### 10.6 Ongoing Relationships with Suspicious Clients

Axum does not maintain relationships where there's a reasonable belief Axum may be used for ML/TF. The RCO/MLRO and senior management decide whether to exit or retain with enhanced monitoring (e.g., tighter limits, EDD refresh, more frequent reviews). If a UTR has been filed, consult FIU Curaçao as/if required before exiting.

#### 10.7 Legal & Regulatory Orders

Orders may include production/disclosure orders, client information orders, account-monitoring orders, search/seizure warrants, or requests for financial information. Immediately forward to the RCO/MLRO, who will liaise with legal counsel and coordinate responses.

## 10.8 Training

Axum provides at least annual training for the RCO/MLRO, deputy(s), and impacted staff on indicators, red flags, case handling, narrative drafting, and goAML reporting. Training is updated upon regulatory change or audit findings.

## 10.9 Record-Keeping

Retain UTRs, internal reports, investigation files, and supporting documentation for at least seven (7) years from report date, or longer if required by law or until notified that any related investigation is closed. (Other records are retained per Axum's broader record-keeping policy and local law.)

## 11.1 Introduction

Given Axum's size and the nature of its business, effective monitoring relies on:

1. Maintaining accurate, up-to-date customer information; and
2. Timely, risk-based enquiries to understand unusual activity and determine if it is reasonable or potentially reportable (see Chapter 10).

Monitoring combines automated controls, structured reviews, and trained staff judgement within Axum's risk appetite and legal obligations.

## 11.2 Keeping Client Information Up-to-Date (Periodic KYC Refresh)

Axum conducts periodic KYC refreshes on a risk basis:

- High risk: at least annually
- Medium risk: every 2–3 years
- Low risk: every 3–5 years

Reviews confirm changes to ownership/control, key management, business lines, geography, products used, source of funds/wealth where relevant, and overall transactional behaviour. Unless the RCO/MLRO directs otherwise, it is not necessary to re-collect all onboarding documents; the refresh is risk-based and targeted to changes.

Trigger events (refresh outside cycle): material ownership or control changes; new higher-risk products/jurisdictions; PEP/sanctions/adverse-media hits; atypical activity; internal risk re-rating; or regulatory updates.

All staff must promptly record client changes on file and notify the RCO/MLRO if risk may be affected. The RCO/MLRO determines whether to re-evaluate risk and accelerate refresh.

### 11.3 Transaction & Behaviour Monitoring

Axum uses a combination of automated and manual controls:

#### A. Automated / rules-based controls (proportionate to scale):

- Velocity/amount thresholds, structuring/smurfing patterns, rapid in-out, layering typologies
- Jurisdiction risk (inbound/outbound), product risk, counterparty/wallet risk (incl. blockchain analytics)
- Sanctions and watchlist screening (pre- and post-event where applicable)
- Behavioural baselines vs. customer economic profile

#### B. Analyst review & escalation:

- Investigate alerts; request clarifications and documentation from the customer when justified
- Consider customer profile, expected activity, source of funds/wealth, and counterparties
- Escalate to the RCO/MLRO if suspicion forms or indicators meet “unusual transaction” criteria (see Chapter 10)

C. What to look for (illustrative):

- Unusual nature: abnormal size/frequency/patterns for the customer segment
- Series effects: repetitive credits/transfers inconsistent with profile
- Geography: high-risk or sanctioned links; opaque routing
- Operating model gaps: non-face-to-face + overseas payouts that cannot be tied to the customer's own account/wallet without good reason

If you have doubts, report to the RCO/MLRO immediately per Chapter 10.

Important: Curaçao has no "consent SAR / 7-day wait" regime. Do not delay or condition payments on "consent." Follow Chapter 10 (UTR via goAML) and any explicit instructions received from FIU/law enforcement.

D. Compliance Monitoring Program (CMP):

- Quarterly sampling to confirm onboarding, screening, due diligence, and monitoring controls were applied as designed
- Findings tracked to remediation; material issues reported to Senior Management and the Board

11.4 Funds Transfer & FATF Travel Rule Compliance

Axum complies with FATF Recommendation 16 for virtual asset (VA) and fiat transfers, as implemented in Curaçao and applicable counterparties' laws.

Threshold & scope

- For VA transfers at or above USD/EUR 1,000, Axum collects and transmits required originator and beneficiary information to the receiving VASP/financial institution.
- Below the threshold, Axum applies risk-based measures (incl. sanctions screening and anomaly checks).

Required information (minimum for qualifying VA transfers):

1. Originator: full legal name; unique identifier (account/wallet/customer ID); and one of: (i) address, (ii) national ID number, or (iii) date and place of birth.
2. Beneficiary: full legal name; unique identifier (account/wallet/customer ID).

Counterparty-VASP due diligence

- Axum confirms the status and legitimacy of the receiving/sending VASP (licensing/registration where applicable, sanctions checks, adverse media, jurisdiction risk).
- Where counterparties cannot reliably receive, protect, and pass Travel Rule data, Axum applies risk-based restrictions (e.g., limit/decline transfer, enhanced verification, additional documentation).

Unhosted/self-custody wallets

- When transacting with unhosted wallets, Axum uses risk-based measures to gain comfort on beneficial ownership/control (e.g., Satoshiproof/signed message, micro-transaction verification, documentary SoF, additional monitoring) and may decline where assurance is inadequate.

Transmission & security

- Transmit required data securely using recognised formats/standards (e.g., IVMS101 or equivalent), protect confidentiality, and retain evidence of successful transmission.
- Screen all transfers against sanctions lists and apply ongoing monitoring.
- If data is missing, unverifiable, or counterparties cannot comply, hold or reject the transfer and escalate to the RCO/MLRO.

Governance

- The RCO/MLRO ensures Travel Rule controls are embedded, tested, and kept current; exceptions are documented with compensating controls.

#### 11.5 Quality Assurance, Model Governance & Tuning

- QA testing: Periodic independent testing of alert logic, sanctions screening efficacy, and case documentation quality.
- Model/Rules governance: Document scenarios, thresholds, data sources, and change control. Tune scenarios at least annually (or upon material events) using production data, with back-testing and false-positive analysis.
- Management Information (MI): Monthly/quarterly KPIs (alerts, dispositions, turnaround times, UTRs filed, repeat alerts, sanctions hits) reported to Senior Management; trends and remediation tracked.

#### 11.6 Record-Keeping

Maintain evidence of monitoring (alerts, reviews, case notes, decisions, communications, data transmissions, and MI/QA results) for at least 7 years from the review date, or longer where required by Curaçao law or until notified any related investigation is closed.

## CHAPTER 12: RECORD RETENTION

### 12.1 Introduction

This Chapter sets out the record-keeping standards that Axum must meet under the Curaçao AML/CTF framework. Maintaining complete and accurate records ensures that Axum can:

- Provide a full audit trail for all advice, instructions, and transactions undertaken on behalf of clients;
- Supply timely and adequate information to law-enforcement and regulatory authorities during investigations;
- Support ongoing monitoring of client activity against expected behaviour;
- Identify and report unusual or suspicious activity; and
- Demonstrate compliance with all statutory and regulatory obligations.

#### 12.2 Scope of Records to Be Kept

Axum must maintain, for each customer and its own operations, records sufficient to verify identity, reconstruct transactions, and evidence compliance. This includes:

- Customer identification/KYC records and verification documentation;
- Business and transaction records for each client relationship;
- Internal and external Unusual Transaction Reports (UTRs) and related correspondence;
- The Resident Compliance Officer (RCO)/MLRO annual report and any other compliance reports;
- Records of training, monitoring, and the effectiveness of AML training; and
- Compliance testing and audit working papers.

Retention of these records does not breach data-protection laws when performed in accordance with legal obligations and Axum's Privacy Policy. Records will be made available without undue delay to competent authorities upon lawful request.

### 12.3 Customer Identification Records

Identification and verification records must be retained for at least seven (7) years after the end of the business relationship, defined as the later of:

- the date of the last transaction; or
- the date the account or relationship was formally closed.

If an investigation or legal proceeding is ongoing, records must be retained until written confirmation is received that the matter is closed.

### 12.4 Transaction Records

All transaction records (fiat or digital-asset) must be kept for at least seven (7) years from the transaction date. Records must provide a satisfactory audit trail enabling the reconstruction of individual transactions, including:

- customer and counterparty identifiers,
- transaction date, amount, currency, and purpose,
- payment or wallet addresses, and
- any related instructions or correspondence.

### 12.5 Third-Party Record Keeping

Where Axum appoints representatives, introducers, or administrators, it remains fully responsible for ensuring they comply with these record-keeping standards.

Outsourcing agreements must:

- Require secure storage and retention of all CDD and transaction data for the statutory period; and
- Grant Axum, its auditors, and competent authorities unfettered access to such records upon request.

#### 12.6 Reliance on and by Third Parties

1. When Axum is relied upon by another entity for CDD:  
Axum retains all customer identification records for at least five (5) years from the date of reliance and provides timely access to the relying entity or supervisory authority on request.
2. When Axum relies on a third party for CDD (Reg. 14 PMLTF):
  - Ensure the third party can immediately provide copies of identification data and documents.
  - Confirm that the third party applies equivalent AML standards and maintains its own statutory retention.
  - Keep written agreements covering access rights and data-protection safeguards.
3. Confidentiality limitations:  
Axum will not enter into reliance or outsourcing arrangements that restrict its or the regulator's access to required records due to confidentiality or data-protection clauses.

#### 12.7 AML/CTF Training Records

Axum retains for at least seven (7) years:

- Training dates;
- Nature, content, and delivery method;
- Names and positions of attendees; and

- Test or assessment results (where applicable).

#### 12.8 Compliance Monitoring and Governance Records

Retain for at least seven (7) years:

- Results of periodic compliance testing and monitoring;
- The annual RCO/MLRO report to the Board and any other reports to senior management; and
- Minutes or records of management consideration and actions arising from those reports.

#### 12.9 Refused or Declined Business Records

When business is refused because the client fails to satisfy KYC/CDD requirements or appears inconsistent with Axum's risk appetite, the reason and supporting documentation must be retained for seven (7) years.

#### 12.10 Wire Transfer and Electronic Payment Records

All electronic payment and blockchain transfer messages must contain sufficient information to identify both the originator and the beneficiary, including:

- Full legal names,
- Addresses or unique identifiers, and
- Account or wallet numbers.  
Where the message format cannot hold full details, Axum will retain the complete information internally and ensure its retrieval on demand (see Chapter 11 – Travel Rule).

#### 12.11 Format, Storage and Retrieval of Records

Axum may store records in original, photocopied, scanned, microfiche, or electronic form, provided authenticity, integrity, and accessibility are preserved. Records may be held offsite or outside Curaçao, subject to:

- Compliance with data-protection and cross-border-transfer requirements; and
- A contractual guarantee that records are accessible within 48 hours upon request by Axum or the competent authority.

Where technically feasible, records will be retained within Axum's secure document-management system located on its business premises or approved cloud environment.

#### 12.12 Sanctions and Penalties

Failure to comply with record-keeping obligations under the PMLTF or related regulations may result in:

- Regulatory censure,
- Administrative or criminal penalties, including fines or imprisonment for responsible persons, and/or
- Internal disciplinary action by Axum

## Chapter 13: SANCTIONS

### 13.1 Introduction (Curaçao Context – Expanded)

This Sanctions Policy ("Policy") establishes Axum's commitment to full compliance with all economic, trade, and financial sanctions laws and regulations applicable in Curaçao and in each jurisdiction where Axum conducts business.

Sanctions are a key element of the global framework for combating money laundering, terrorist financing, proliferation financing, corruption, and other threats to international security.

In Curaçao, sanctions obligations arise primarily from:

- United Nations Security Council (“UNSC”) Resolutions adopted by the Kingdom of the Netherlands and directly applicable to Curaçao;
- European Union (“EU”) restrictive measures, which the Kingdom implements through Kingdom Decrees and publishes in the National Gazette of the Netherlands and Curaçao Gazette;
- Local measures and guidance issued or enforced by the Curaçao Gaming Authority (CGA) and the Central Bank of Curaçao and Sint Maarten (CBCS); and
- Extra-territorial sanctions programs administered by partner jurisdictions with which Axum interacts commercially (including the United States Office of Foreign Assets Control (OFAC), the UK Office of Financial Sanctions Implementation (OFSI), and similar competent authorities).

Accordingly, Axum (“the Company”) maintains this Policy to ensure that no part of its gaming, payment-processing, or digital-asset exchange activities is used to circumvent or violate these regimes.

This Policy applies to all directors, officers, employees, consultants, contractors, and third-party agents (“Covered Persons”) acting on behalf of the Company, regardless of location.

#### Purpose and Governance

The objective of this Policy is to:

- Embed sanctions compliance within Axum’s governance and risk-management framework;
- Provide clear standards, responsibilities, and controls for identifying, screening, and managing sanctions exposure; and
- Protect the Company, its clients, and its employees from the legal, regulatory, and reputational risks of non-compliance.

Axum’s Resident Compliance Officer (RCO)/Money Laundering Reporting Officer (MLRO) is responsible for implementing this Policy, monitoring adherence, and liaising with the CGA, the CBCS, and relevant international bodies.

### Applicability and Scope

This Policy covers every Axum business line, including but not limited to:

- Online gaming and player-account services (e.g., deposits, winnings withdrawals, and payouts);
- Payment processing and settlement services, whether fiat or digital assets;
- Any wallet, exchange, or custodial functionality operated or outsourced under a CGA-approved T-Licence or equivalent authorization; and
- All vendor, affiliate, and marketing arrangements where funds or value may be transferred.

### General Obligation

Covered Persons must:

1. Comply with all applicable sanctions laws and regulations, including the blocking of property or rejection of transactions involving designated persons or jurisdictions;
2. Refrain from any facilitation of activities that would breach sanctions, whether directly or indirectly;
3. Conduct risk-based screening of customers, counterparties, and transactions against the consolidated sanctions lists of the UN, EU, UK (HM Treasury), OFAC, and CGA; and
4. Immediately escalate to the RCO/MLRO any potential match, red flag, or suspicion of sanctions evasion.

No Covered Person is authorized to transact, approve, or otherwise engage in business that contravenes sanctions requirements.

Axum also prohibits any person from authorizing or directing another to perform a prohibited act, or from concealing information to avoid sanctions detection.

### Sanctions Dynamics

Sanctions programs evolve rapidly in response to geopolitical events. Covered Persons are expected to remain informed of new or amended measures and to follow the latest internal communications and compliance alerts issued by the RCO/MLRO.

Failure to comply with this Policy may expose both the Company and individuals to civil and criminal penalties, including fines, imprisonment, and regulatory censure.

Axum's leadership affirms its zero-tolerance approach to sanctions breaches and its commitment to uphold the highest international standards of integrity, transparency, and good governance consistent with Curaçao's obligations under the United Nations, European Union, and CGA/CBCS frameworks.

### 13.2 Policy Statement

Sanctions are implemented through laws, regulations, and decrees issued by competent authorities at the international, Kingdom, and national levels. In Curaçao, these measures are primarily derived from the United Nations Security Council ("UNSC") Resolutions, the European Union ("EU") restrictive measures, and their implementation through Kingdom Decrees on Sanctions, which extend to Curaçao by virtue of the Charter for the Kingdom of the Netherlands (Statuut voor het Koninkrijk der Nederlanden).

Supervisory responsibility for sanctions implementation and enforcement rests with the Curaçao Gaming Authority ("CGA") for gaming and virtual-asset licensees, and with the Central Bank of Curaçao and Sint Maarten ("CBCS") for financial institutions and payment service providers. Both agencies require license holders to establish and maintain an effective Sanctions Compliance Programme as part of their overall AML/ATF framework.

Accordingly, Axum ("the Company") and all directors, officers, employees, contractors, and agents ("Covered Persons") must comply fully with:

- The United Nations sanctions lists, as adopted and implemented in Curaçao;
- The European Union Consolidated Financial Sanctions List;
- The UK Office of Financial Sanctions Implementation (OFSI) list;
- The U.S. Office of Foreign Assets Control (OFAC) Specially Designated Nationals (SDN) list, where dealings have U.S. nexus; and
- Any CGA or CBCS-issued lists or directives implementing or extending these obligations domestically.

Each sanctions program may differ in its scope and coverage, but they generally restrict access to certain markets or prohibit transactions involving designated individuals, entities, assets, or jurisdictions. Many programs require entities to block (freeze) property belonging to, or controlled by, designated persons, and to refrain from making any funds or economic resources available to them.

It is therefore illegal — and contrary to Company policy — to engage in any business or transaction with a person or entity named on a sanctions list, or with any entity that is 50 percent or more owned, directly or indirectly, by one or more designated persons.

If any individual or entity with whom Axum conducts business is subsequently added to a sanctions list, all related business must immediately cease, and the Resident Compliance Officer (RCO)/Money Laundering Reporting Officer (MLRO) will issue written instructions on the handling or freezing of related assets and funds. No action may be taken by any Covered Person without the prior approval of the RCO/MLRO.

Sanctions regimes are dynamic and can change rapidly in response to global political developments. Covered Persons are expected to remain vigilant and ensure that all customers, vendors, and counterparties are screened and cleared prior to onboarding and throughout the business relationship. Questions or uncertainties must be referred promptly to the RCO/MLRO.

Violations of applicable sanctions laws can attract severe civil, administrative, and criminal penalties, including fines, imprisonment, and loss of licence. Each Covered Person must immediately report to the RCO/MLRO any known or suspected sanctions breach, attempted transaction, or communication involving a sanctioned person or jurisdiction.

Axum's Sanctions Policy forms an integral part of its risk-based AML/ATF framework. The Policy, associated procedures, and internal controls are designed to ensure continuous compliance with Curaçao's domestic obligations and the broader Kingdom's international commitments. While the Compliance Department will update procedures to reflect regulatory changes, every Covered Person remains responsible for maintaining awareness of current sanctions developments.

The Company's leadership reaffirms a zero-tolerance approach to sanctions violations and is committed to fostering a culture of ethical conduct and compliance across all business lines.

### 13.3 Sanctions Programmes

Numerous international authorities administer sanctions programmes that restrict dealings with specific countries, territories, individuals, sectors, and activities. These programmes serve foreign-policy and national-security purposes by blocking assets, restricting trade, and preventing the flow of funds to prohibited parties.

The primary sanctions frameworks applicable to Axum include:

- United Nations Security Council (UNSC) measures implemented through Kingdom Decrees on Sanctions (Sanctieregelingen Curaçao);
- European Union Restrictive Measures, directly applicable within the Kingdom and periodically updated via the Official Journal of the EU;
- CGA and CBCS Directives implementing UN/EU measures and providing practical guidance to licensees; and
- Other foreign programmes (e.g., OFAC, OFSI, Global Affairs Canada) to the extent that Axum's operations, counterparties, or financial flows have exposure to those jurisdictions.

#### Lists of Designated Persons and Entities

International and domestic authorities maintain public lists of individuals, entities, and vessels with whom dealings are restricted or prohibited. Because these lists are updated frequently, all Covered Persons must confirm — prior to any transaction — that the parties involved are not subject to applicable sanctions.

Screening (or “sanctions checking”) shall be conducted using:

- A commercial sanctions-screening platform integrated with the UN, EU, UK, US, and CGA consolidated lists; or
- Official consolidated lists issued by the relevant authorities, where manual checks are required.

Covered Persons responsible for onboarding or payments must be trained to conduct such screening effectively and to recognise potential matches. The RCO/MLRO shall ensure that sanctions-screening tools are regularly updated, tested for accuracy, and capable of detecting both direct and indirect ownership or control relationships.

If a name or entity returns a potential match, the following must occur:

1. The match must be immediately escalated to the RCO/MLRO.
2. The RCO/MLRO will verify the match using reliable information sources and determine whether to block, reject, or proceed with the transaction.
3. If blocking or rejection is required under Curaçao law or Kingdom Decree, the RCO/MLRO will report the matter without delay to the CGA and, if applicable, to the Financial Intelligence Unit Curaçao (FIU Curaçao), following prescribed reporting timelines and formats.
4. All documentation, correspondence, and decisions shall be retained for a minimum of five (5) years in accordance with Chapter 12 (Record Retention).

Axum shall not enter into or continue any business relationship with persons or entities appearing on applicable sanctions or restrictive-trade lists. Where assets or funds are held on behalf of a sanctioned person, Axum will immediately freeze such assets in accordance with relevant laws and ensure the RCO/MLRO documents the action taken.

Where required, the RCO/MLRO will submit a Blocked- or Rejected-Transaction Report to the CGA, CBCS, or other competent authority within the timeframe specified by law or guidance.

#### 13.4 Jurisdictions Subject to Comprehensive Embargoes

Sanctions authorities (including the United Nations and the European Union) periodically impose comprehensive or near-comprehensive measures against certain countries/territories and sectoral measures against others. These measures are dynamic and may change at short notice.

Axum does not conduct business with customers, counterparties, or vendors that:

- are established in, located in, or ordinarily resident in jurisdictions subject to comprehensive embargoes under UN/EU measures as implemented within the Kingdom;
- are owned or controlled (directly or indirectly) by designated persons; or
- seek to route transactions to, from, or through such jurisdictions.

Because lists change frequently, Axum does not maintain a static list in this Policy. Instead, the RCO/MLRO ensures screening tools are updated daily (or near-real-time) with the UN and EU consolidated lists, UK OFSI, US OFAC (where nexus exists), and CGA/CBCS directives.

Geofencing & location controls. To enforce jurisdictional restrictions, Axum uses proportionate controls, for example:

- IP geoblocking; device and SIM metadata checks (where lawful);
- payment rail country checks (issuer/acquirer BIN, IBAN/BIC);
- document-issuing country and residence consistency checks; and
- step-up verification for anomaly patterns (e.g., VPN/Tor indicators).

Where uncertainty exists, the relationship or transaction is declined or blocked pending RCO/MLRO determination.

### 13.5 Facilitation

“Facilitation” includes any direct or indirect action that assists, enables, or conceals dealings that would breach applicable sanctions. Covered Persons must not:

- refer prohibited opportunities to third parties to circumvent Axum’s obligations;
- alter processes/records to avoid detection;
- provide approvals that would permit a prohibited transaction; or
- structure transactions to obscure a sanctioned nexus (e.g., intermediary wallets, pass-through accounts, or layered vendor chains).

This prohibition also applies to extra-territorial risk (e.g., asking a non-Curaçao affiliate or vendor to do what Axum cannot lawfully do). When in doubt, escalate to the RCO/MLRO before taking any action.

### 13.6 No Grandfathering

Sanctions typically take effect immediately upon legal adoption and apply to existing as well as future dealings. If a current customer, vendor, asset, wallet address, or jurisdiction becomes sanctioned:

- Stop new dealings and freeze or reject activity based on the applicable regime;
- Seek guidance from the RCO/MLRO on wind-down, freezing obligations, or licence applications;
- Do not undertake any “unwind” without the RCO/MLRO and legal counsel’s written approval.  
Where a licence or exemption is required to wind down or release funds, Axum will wait for written authorisation from the competent authority.

### 13.7 Compliance Procedures

Axum’s Sanctions Compliance Programme is risk-based and includes:

- Governance & Accountability: Board oversight; RCO/MLRO ownership; clear roles for onboarding, payments, vendor management, and tech.
  - Risk Assessment: Business-wide and product-specific sanctions risk assessments reviewed at least annually or upon trigger events.
  - Internal Controls: Policies, screening standards, name and transaction screening (including wallet screening where applicable), escalation paths, case management, and document retention.
  - Technology & Data: Approved screening tools, daily list updates, fuzzy-match logic, ownership/control evaluation, and robust audit trails.
  - Testing & Assurance: Periodic QA and independent testing (internal audit or external) with tracked remediation.
  - Training: Role-based initial and annual training; targeted refreshers after regulatory updates or incidents.
-

### 13.8 Identifying Sanctions Compliance Risk

Pre-engagement and ongoing screening is required for all relevant parties (customers, UBOs, directors, signatories, vendors, affiliates, and key counterparties).

#### i) Sanctions Risk Assessment Evaluate:

- Customer risk: PEPs, complex ownership, higher-risk industries, and jurisdictional exposure;
- Products/services: cross-border payments, digital assets or wallets (if applicable), and cash-like features;
- Activity risk: volumes, velocity, patterns suggesting evasion;
- Channels: non-face-to-face, agents/introducers, and third-party processors;
- Geography: sanctioned or high-risk jurisdictions;
- Systems/processes: efficacy of screening tools, coverage of transliteration/aliases, and performance metrics.

#### ii) Sanctions List Screening Procedures

- Lists: UN, EU, UK OFSI, US OFAC (where nexus exists), and CGA/CBCS directives.
- Frequency:
  - Onboarding (prior to approval),
  - Ongoing (periodic batch + event-driven),
  - Real-time/near-real-time for payments and withdrawals where feasible.

- Tools: Use approved third-party tools with:
  - daily consolidated list updates;
  - strong fuzzy-matching;
  - ownership/control evaluation (≥50% direct/indirect rule and “control” indicators);
  - documentable dispositions (true/false positives) and case evidence.
- Transaction screening: Names, IBAN/BIC, beneficiary/originator details, narrative fields; wallet address screening where Axum handles crypto.
- Event-driven re-screening: changes in name, address, UBOs, directors, control, or adverse news; new designations; list updates; or alerts indicating evasion typologies.

### iii) Governance and Reporting

- All potential matches are immediately escalated to the RCO/MLRO.
- The RCO/MLRO determines whether to block/freeze or reject, and whether to notify the CGA and/or CBCS and, where the activity is unusual, to file a UTR with FIU Curaçao (see Chapter 10).
- Maintain a Sanctions Case Register with outcomes, reports filed, and retained evidence (see Chapter 12).

### 13.9 Licences

In limited cases, transactions otherwise prohibited may be permitted under a general or specific licence issued by a competent authority (e.g., EU national competent authority via the Kingdom; OFSI for UK nexus; OFAC for U.S. nexus).

- General Licences: Pre-authorised categories of activity. Covered Persons must confirm that all conditions are satisfied and obtain RCO/MLRO + Legal approval before proceeding.

- Specific Licences: Case-by-case approvals. Only the RCO/MLRO, with Legal, may submit applications. No action is taken until the licence is received in writing and validated; conditions must be tracked and strictly observed.

Axum maintains a Licence Register (applications, approvals, conditions, expiries, reports due).

#### 13.10 Reports and Records

Where a block or reject is required, the RCO/MLRO will file any required notifications with the CGA and/or CBCS and, where applicable, the Kingdom's designated competent authority (and OFSI/OFAC if a UK/U.S. nexus applies). If the activity also meets unusual transaction indicators, a UTR will be filed with FIU Curaçao per Chapter 10.

Axum keeps sanctions records for at least five (5) years from the later of the event or authorisation expiry, and otherwise in line with Chapter 12 (minimum seven years for core AML records). Records include:

- Reports filed (blocked/rejected, regulator correspondence);
- Copies of licences and submissions;
- Screening evidence (hits, dispositions, ownership analysis);
- Case files, narratives, approvals, and audit trail.

#### 13.12 Training

All Covered Persons complete annual sanctions training appropriate to their role. At minimum, training covers:

- UN/EU frameworks and CGA/CBCS expectations;
- List types, 50% ownership/control concepts, and evasion typologies;
- How to use Axum's screening tools;

- Block vs reject decisions, escalation to the RCO/MLRO, and reporting flows;
- Wallet/address screening (if Axum handles crypto);
- Record-keeping and confidentiality requirements.

Attendance and assessments are recorded per Appendix 2 (AML Course Register) and Chapter 12.

#### 13.13 Responsible Individual

The Resident Compliance Officer (RCO)/MLRO is responsible for day-to-day sanctions compliance, including:

- Maintaining the programme, tools, and procedures;
- Advising staff, reviewing matches, and deciding block/reject actions;
- Filing required notifications (CGA/CBCS/competent authorities) and UTRs where applicable;
- Overseeing training, QA/testing, and remedial actions;
- Providing periodic MI to Senior Management and the Board.

#### 13.14 Sanctions Violations

Breaches of applicable sanctions may result in civil/administrative penalties, criminal sanctions, licence conditions, or revocation. Axum will consider voluntary disclosures to the relevant competent authority where appropriate, guided by counsel.

Internally, violations are subject to disciplinary action up to and including termination. All staff must immediately inform the RCO/MLRO of suspected breaches or attempted sanctions-evasion activity.

#### 13.15 Handling Blocked Property and Rejected Transactions

Blocked (frozen) property arises where law requires Axum to immobilise funds/economic resources of a designated person. Rejection applies where Axum must refuse a prohibited transaction but no blocking obligation exists.

Operational steps (minimum):

1. Immediate action: Suspend processing; secure the asset/funds; prevent movement.
2. Classification: RCO/MLRO determines block vs reject under the applicable regime (UN/EU/UK/US nexus).
3. Segregation & records: For blocks, segregate funds in a restricted internal account; record identifiers (account/wallet, TX hash, timestamps, currency), and retain statements.
4. Interest/returns: Apply interest or equivalent treatment only if required/permitted by the relevant regime; never make funds available to designated persons.
5. Notifications: File required block/reject reports with the CGA/CBCS and the competent authority, and (if unusual) file a UTR with FIU Curaçao.
6. Customer communication: Provide neutral, non-tipping messaging approved by the RCO/MLRO; do not disclose list status or internal filings unless legally required.
7. Ongoing review: Monitor for de-listing/licensing changes; update case status and report when assets are lawfully unblocked or released under licence.
8. Registers: Maintain Blocked Property and Rejected Transaction registers, reconcile them monthly, and retain evidence per Chapter 12.

Crypto-specific note (if applicable): Where Axum handles digital assets, block by restricting the internal ledger position (not on-chain transfer), label addresses as restricted, and prevent withdrawals. Record wallet addresses, TXIDs, and blockchain analytics references in the case file.

## Chapter 14: Governance and Oversight

### 14.1 Senior Management Responsibilities and Governance

Senior management plays a central role in ensuring the effectiveness of Axum's Anti-Money Laundering and Anti-Terrorist Financing ("AML/ATF") framework. They are responsible for promoting a culture of compliance, approving and maintaining robust policies, providing adequate resources, and exercising continuous oversight of all AML/ATF activities. In line with Regulation 2 of the Curaçao AML/ATF Regulations, senior management comprises those who exercise executive control and decision-making authority within the Company.

Management reviews and approves the Company's AML/ATF policies and procedures at least annually or whenever regulatory or operational changes occur. It ensures that a risk-based approach is consistently applied by supporting periodic risk assessments and the implementation of proportionate controls. Senior management must provide sufficient human, technological, and financial resources to the Resident Compliance Officer ("RCO") / Money Laundering Reporting Officer ("MLRO") and oversee their performance while preserving independence and authority. Compliance reports, internal audit findings, and identified deficiencies are reviewed promptly and remediated within agreed timelines.

The governance framework approved by management must align with the expectations of the Curaçao Gaming Authority ("CGA") and clearly set out reporting lines, escalation channels, and accountability for AML/ATF oversight. All members of management are expected to complete AML/ATF training to remain informed about their regulatory obligations, emerging financial-crime risks, and supervisory developments.

Axum's senior management team currently includes:

### ADD DETAILS

SBC Corporate Services Ltd. as the appointed corporate service provider. External advisors and legal or compliance consultants may be engaged as necessary to ensure that the Company's policies and procedures remain consistent with Curaçao and international best practices.

The Resident Compliance Officer is appointed at managerial level and reports directly to senior management and the Board of Directors. The RCO/MLRO has the autonomy to oversee the AML/ATF compliance program and escalate issues of material significance directly to the Board. Axum provides the RCO/MLRO with initial and ongoing training on the Company's AML/ATF framework, relevant laws, and international standards. All training activities are documented and reviewed by management to confirm continuing competence. An organizational chart depicting governance and reporting lines is maintained as part of the Company's internal controls.

## 14.2 Independent Audit Function

In accordance with Regulation 17A(1) and (2) of the Curaçao AML/ATF Regulations, Axum ensures that its AML/ATF program is independently reviewed at least once each year. The audit may be performed by an external specialist with relevant expertise or by internal personnel who are independent of the compliance function to preserve objectivity.

The audit provides an impartial assessment of the Company's AML/ATF risk management, internal controls, and compliance functions. Its scope and methodology are approved by the RCO/MLRO and presented to the Board for endorsement. The resulting report, including findings and recommendations, is submitted to senior management and the Board. Corrective actions are documented, tracked, and completed within reasonable timeframes to demonstrate ongoing improvement. Where significant issues are identified, management will promptly inform the CGA and take remedial measures consistent with the regulator's expectations.

### 14.3 Branches and Subsidiaries

Axum currently conducts operations solely within Curaçao. However, in recognition of its obligations under Regulations 12 and 12A of the AML/ATF Regulations, the Company will ensure that equivalent AML/ATF standards are implemented should branches or subsidiaries be established abroad.

Any future foreign operations must apply AML/ATF measures consistent with Curaçao's legal framework, including the application of a risk-based approach, group-wide policies, and procedures for suspicious-activity reporting. The Company will maintain effective oversight of such entities to ensure that their controls and compliance programs mirror the standards required under Curaçao law and that reports of suspicious activities are submitted both to the local Financial Intelligence Unit and to FIU Curaçao when appropriate.

Before opening in any higher-risk jurisdiction, Axum will notify the CGA and assess the need for additional safeguards or enhanced monitoring. This policy will be reviewed at least annually or when structural or operational changes occur to ensure continuing alignment with regulatory obligations.

### 14.4 Annual Review and Board Reporting

Each year, senior management and the Board of Directors conduct a comprehensive review of the AML/ATF program to evaluate its effectiveness and alignment with current regulations and business activities. The RCO/MLRO prepares an Annual Compliance Report summarizing monitoring results, internal audit findings, training completion, key risk developments, and any material regulatory correspondence.

The Board reviews and approves updates to the AML/ATF policy, annual risk assessment outcomes, and remediation plans. Meeting minutes, reports, and supporting documentation are maintained in accordance with Chapter 12 (Record Retention). Where requested, the Annual Compliance Report and associated materials are provided to the CGA as evidence of oversight.

This review process reinforces the Board's accountability for AML/ATF compliance and ensures that governance, resources, and internal controls remain proportionate to Axum's risk profile and regulatory environment.

#### APPENDICES – INDEX

##### Appendix 1 – Suspicious Transaction Reporting (STR) Form

Standard internal form for staff to report suspicions to the RCO/MLRO, with an RCO/MLRO section for disposition and FIU Curaçao filing notes; includes pre-/post-transaction handling and anti-tipping-off reminder.

Appendix 2 – AML Course Register of Attendees

Attendance and attestation record for AML/ATF training; captures names and signatures. Training records retained per Chapter 12.

Appendix 3 – Proof Documents for Natural Persons

Acceptable identification and address-verification evidence where electronic checks are insufficient; includes government photo ID and supporting documents from FATF-equivalent jurisdictions.

Appendix 4 – Sample Red Flags

Illustrative indicators of unusual or suspicious activity across customer behaviour, documentation, transactions, geography, virtual-asset and PEP contexts. All red-flagged activity must be escalated immediately to the RCO/MLRO.

Appendix 5 – Useful Information Sources

Primary national and international references supporting AML/ATF and sanctions compliance, including:

- Financial Intelligence Unit Curaçao (FIU Curaçao) <https://www.fiucuracao.cw>
- Curaçao Gaming Authority (CGA) <https://www.curacaogamingauthority.com>
- Central Bank of Curaçao and Sint Maarten (CBCS) <https://www.centralbank.cw>
- Financial Action Task Force (FATF) <https://www.fatf-gafi.org>
- UN Security Council / EU / OFAC Sanctions Lists

Appendix 6 – Summary of Existing Laws

Key Curaçao AML/ATF instruments:

- National Ordinance on Identification for Financial Services (LOK)
- National Ordinance on the Reporting of Unusual Transactions (NORUT)
- AML/ATF Regulations 2008
- CGA / CBCS Guidelines and sectoral notices.

Appendix 7 – Anti-Money Laundering Manual Declaration

Employee acknowledgement of having read, understood, and agreed to comply with the Manual; retained in the compliance file for audit verification.

Appendix 8 – Enhanced Due Diligence (EDD) Report Template

Structured template for documenting high-risk reviews: ownership and control, source of funds/wealth, geography, transactional behaviour, adverse media, conclusions, and recommendations. Records retained for seven years after relationship end.

Appendix 9 – Customer Risk Identifiers

Matrix of inherent risk factors for individuals, corporates, account opening/servicing channels, and high-risk categories. High-risk customers (e.g., PEPs, VASPs, casinos) subject to EDD and annual review.

*(For insertion of the table, use Table Grid format with three columns: Category | Risk Factors | Examples / EDD Triggers.)*

Appendix 10 – AML Compliance Trigger Events

Operational triggers (e.g., transaction anomalies, high-risk jurisdictions, structuring, PEP involvement, or negative news) that require documentation, RCO/MLRO assessment, and potential STR escalation to the FIU Curaçao.

APPENDIX 1 – SUSPICIOUS TRANSACTION REPORTING (STR) FORM – MONEY LAUNDERING

Name of Person Reporting a Suspicion: \_\_\_\_\_  
Job Title / Responsibility: \_\_\_\_\_  
Client Name & Address: \_\_\_\_\_  
Details of Event(s) Giving Rise to Suspicion: (attach separate sheet if needed)

Details of Supporting Evidence Attached (if any): \_\_\_\_\_  
Is this report being made pre- or post-transaction? \_\_\_\_\_  
Signature / Date: \_\_\_\_\_

The employee shall submit this completed form to the Resident Compliance Officer (RCO) / Money Laundering Reporting Officer (MLRO) immediately and retain a personal copy for record purposes.

To be Completed by Resident Compliance Officer (RCO) / MLRO

Client Name: \_\_\_\_\_  
Date Received: \_\_\_\_\_ Date Review Completed: \_\_\_\_\_

- ☐ Yes – copy of the disclosure filed with the Financial Intelligence Unit Curaçao (FIU Curaçao) is attached.  
☐ No – basis for non-disclosure is noted in comments above.

If disclosure is made prior to execution of the transaction, appropriate measures must be taken to ensure the transaction does not proceed for the next seven (7) working days or until clearance is received from FIU Curaçao.

RCO/MLRO Signature / Date: \_\_\_\_\_

*Note – Under Regulation 7 of the Curaçao AML/ATF Regulations, employees must not disclose to any person involved in the transaction that a report has been or will be made (“tipping-off”).*

---

## APPENDIX 2 – AML COURSE REGISTER OF ATTENDEES

Date: \_\_\_\_\_ Course: Anti-Money Laundering & Counter-Terrorist Financing Training

By signing below, you confirm (1) your attendance and (2) that you have understood the content covered.

Name      Signature

Training records shall be retained for at least seven (7) years in accordance with Chapter 12 (Record Retention).

---

## APPENDIX 3 – PROOF DOCUMENTS FOR NATURAL PERSONS

When electronic verification cannot be completed, one or more of the following documents may be used to verify a natural person’s identity.

Government-issued photo identification (must be valid):

- Passport
- Photo-card driving licence (full or provisional)
- National identity card

Additional supporting documents (include but not limited to):

- Current bank or credit card statement from a regulated financial institution in Curaçao, the Netherlands, the EU or any FATF-equivalent jurisdiction (not internet printouts)
- Recent utility bill showing current address

- Instrument of court appointment (e.g. grant of probate or liquidator's order)
- Current municipal or tax assessment letter

*Electronic verification may be accepted where the data source is independent, reliable, and capable of verifying identity to an equivalent standard.*

---

#### APPENDIX 4 – SAMPLE RED FLAGS

The following are examples of potential red-flag indicators of suspicious or unusual activity. The presence of one or more does not automatically imply suspicion, but unexplained occurrences must be escalated for review.

##### General Indicators

- Customer admits or hints at criminal activity.
- Customer requests no correspondence to registered address.
- Customer offers unnecessary explanations for transactions.

##### Documentation and Behavioural Concerns

- Vague or false information provided.
- Documents appear forged or implausible.
- Customer refuses or delays providing identification.
- Attempts to avoid AML procedures or questions.

##### Transactional Anomalies

- Activity inconsistent with business profile.
- Unusually large or complex transactions.
- Transfers to/from high-risk jurisdictions without rationale.

##### Customer Information Issues

- Unverifiable details or frequent changes to wallets/accounts.

- Reluctance to disclose beneficial owners or source of funds.
- Over-explanation or attempt to influence staff.
- Negative media association.

Virtual Asset and Technical Indicators

- Funds sent to addresses linked to dark-web markets or mixers.
- Use of VPN or TOR to conceal location.
- Encrypted email domains (e.g. ProtonMail, Tutanota).

Politically Exposed Persons (PEPs)

- Declared assets inconsistent with public income.
- Access to state funds or monopolies.
- Downplays importance of role or from mono-economy state.

*All red flags must be reported immediately to the RCO/MLRO for determination whether an STR is required.*

---

APPENDIX 5 – USEFUL INFORMATION SOURCES

National Authorities

- Financial Intelligence Unit Curaçao (FIU Curaçao) – <https://www.fiucuracao.cw>
- Curaçao Gaming Authority (CGA) – <https://www.curacaogamingauthority.com>
- Central Bank of Curaçao and Sint Maarten (CBCS) – <https://www.centralbank.cw>

International References

- Financial Action Task Force (FATF) – <https://www.fatf-gafi.org>
- United Nations Security Council Sanctions Lists
- European Union Consolidated Financial Sanctions List
- Office of Foreign Assets Control (OFAC), U.S. Department of the Treasury

Axum maintains access to updated sanctions lists and regulatory databases through its sanctions screening system.

---

#### APPENDIX 6 – SUMMARY OF EXISTING LAWS

Applicable Curaçao AML/ATF laws and guidelines include:

- Curaçao Anti-Money Laundering and Anti-Terrorist Financing Regulations 2008
  - National Ordinance on the Reporting of Unusual Transactions (NORUT)
  - National Ordinance on Identification for Financial Services (LOK)
  - CGA / CBCS Guidelines and sectoral AML notices
- 

#### APPENDIX 7 – ENHANCED DUE DILIGENCE (EDD) REPORT FOR AML PURPOSES

Client Name: \_\_\_\_\_ Client ID: \_\_\_\_\_ Date: \_\_\_\_\_ Prepared by: \_\_\_\_\_

1. Introduction Purpose of EDD review for higher-risk relationships.
  2. Reason for EDD Triggers include high-risk jurisdiction, PEP status, unusual transactions, adverse media, complex ownership.
  3. Client Profile Include key identifiers, source of wealth, and relationship overview.
  4. Detailed Risk Assessment Ownership, Funds/Wealth, Geography, Transaction Behaviour, Adverse Media.
  5. Conclusion and Recommendations Summarise findings and risk rating; recommend retain/restrict/exit/report.
  6. Documentation and Record Keeping List supporting documents; retain for seven (7) years post-relationship.
-

## APPENDIX 8 – CUSTOMER RISK IDENTIFIERS

| Category          | Risk Factors                                              | Inherent Risk | Examples Considered High Risk (EDD Applicable)       |
|-------------------|-----------------------------------------------------------|---------------|------------------------------------------------------|
| Individuals       | Retail (domestic), employed                               | Low           |                                                      |
|                   | Self-employed professional                                | High          | Real estate agents, high-value goods dealers         |
|                   | Foreign PEPs / Non-residents / High-net-worth individuals | High          |                                                      |
| Corporates        | Unregistered partnerships or trusts                       | High          | Intermediaries, private companies with bearer shares |
|                   | Virtual Asset Service Providers (VASPs)                   | High          |                                                      |
|                   | Casinos (including internet gaming)                       | High          |                                                      |
|                   | Cash-intensive businesses                                 | Medium–High   | Retail, restaurants, fuel stations                   |
| Account Opening   | Non-face-to-face or via third parties                     | High          |                                                      |
| Account Servicing | Online or mobile-only channels                            | High          |                                                      |

All high-risk customers are subject to Enhanced Due Diligence and annual review by the RCO/MLRO.

## APPENDIX 9 – AML COMPLIANCE TRIGGER EVENTS

Trigger events require enhanced review or potential reporting under the AML/ATF framework. Examples include:

- Transaction exceeds expected pattern without documented source of funds.
- Sudden increase in activity inconsistent with history.
- Dealings with high-risk jurisdictions or entities.
- Contradictory identification information.
- Multiple small cash deposits suggesting structuring.
- Involvement of PEPs or their associates.
- International transfers to/from weak AML countries.
- Frequent changes to account beneficiaries or details.
- Transactions in high-risk industries (e.g. casinos, unregulated digital platforms).
- Negative media reports relating to financial crime or sanctions.

All trigger events must be recorded and assessed by the RCO/MLRO and, where appropriate, escalated to the FIU Curaçao through a Suspicious Transaction Report (STR).

---

APPENDIX 10 – ANTI-MONEY LAUNDERING MANUAL DECLARATION

I hereby acknowledge that I have read and understood the provisions of the Axum Anti-Money Laundering Manual.

I agree to comply with all policies and procedures contained in the Manual. If unsure about any requirement, I will consult the Resident Compliance Officer (RCO) / MLRO.

I understand that breaches of the Manual may result in criminal prosecution, regulatory censure, or disciplinary action.

Name: \_\_\_\_\_ Signature: \_\_\_\_\_ Date: \_\_\_\_\_

This declaration will be retained in the employee's compliance file for audit purposes.