

Orakum N.V. (141651)

Abraham Mendez Chumaceiro Boulevard 03, Curaçao).

AML/CTF/CPF POLICY

April 2025

Responsible Compliance Officer	Approved by the Board of Directors
Fomenko Volodymyr compliance@orakum-nv.com	Signature: 

Contents

Responsible Compliance Officer.....	1
Approved by the Board of Directors.....	1
Fomenko Volodymyr compliance@orakum-nv.com.....	1
Signature:.....	1
Glossary.....	2
1. Introduction.....	4
2. Abbreviations and Definitions.....	5
3. Overview of the iGaming Regulatory Environment.....	7
4. Money Laundering, Terrorism Financing & Proliferation Financing.....	8
5. Sanctions Adherence and Compliance Framework.....	10
6. Risk-Based Compliance Framework.....	11
6.1 Risk Factors	12
6.2 Technological Developments Risk Assessment	14
7. Due Diligence.....	15
7.1. Comprehensive Customer Due Diligence Measures	15
7.2. Player Identity Verification Process	15
7.3. Understanding the Business Relationship	16
7.4. Ongoing Monitoring and Compliance Oversight	16
7.5. Simplified and Enhanced Due Diligence	17
7.6. Timing of Due Diligence Procedures	18
7.7. Due Diligence for Existing Clients	18
7.8. Termination of Customer Relationships	19
7.9. Third-Party Reliance in CDD Processes	19
8. Suspicious Activity Reporting.....	19
Identifying Unusual Transactions	20
Transaction Types Subject to Reporting	20
Confidentiality in Reporting	21
9. Designated Compliance Officer.....	21
10. Independent Audit.....	22
11. Management Responsibilities.....	24
12. Training & Record Keeping.....	25

Glossary

1. **Account Suspension** – A temporary restriction placed on a player's account, preventing access to gambling activities and transactions.
2. **Affiliate Marketing** – A form of advertising where third-party partners promote an operator's gambling services in exchange for commissions.
3. **Anti-Money Laundering (AML)** – Regulatory measures designed to prevent financial crimes such as money laundering and fraud within the gaming industry.
4. **Betting Limits** – Predefined restrictions on the amount a player can wager over a specific period to promote responsible gaming.
5. **Compliance Officer** – A designated individual responsible for ensuring adherence to legal and regulatory gaming requirements.
6. **Cooling-Off Period** – A short-term gambling restriction (e.g., 24 hours, 7 days, or 1 month) that allows players to take a voluntary break from gaming without permanent account closure.
7. **Deposit Limits** – A responsible gaming feature that enables players to set daily, weekly, or monthly caps on the amount they can deposit into their gaming accounts.
8. **Exclusion Register** – A database of players who have opted for self-exclusion, ensuring they are prevented from accessing gambling services for a specified duration.
9. **Fraud Prevention Measures** – Security protocols used to detect and prevent unauthorized activities, such as multiple account registrations or identity fraud.
10. **Gaming Control Board (GCB)** – The regulatory authority overseeing gaming operations and ensuring compliance with gambling laws in Curaçao.
11. **Know Your Customer (KYC)** – A mandatory verification process requiring players to provide identification documents to confirm their identity and prevent fraudulent activities.
12. **Marketing and Advertising Restrictions** – Guidelines that prohibit the promotion of gambling services to minors, problem gamblers, or vulnerable groups.
13. **National Self-Exclusion Scheme** – A government-regulated program that allows players to self-exclude from multiple gambling operators simultaneously.
14. **Player Risk Profile** – A classification system that assesses a player's gambling behavior to determine their risk level and implement appropriate safeguards.
15. **Problem Gambling** – A condition in which gambling behavior negatively affects a player's personal, financial, or social well-being.
16. **Reality Check Alerts** – Periodic notifications that inform players about the duration of their gaming session, total wagers, and current wins or losses.

17. **Responsible Gaming Officer (RGO)** – A designated staff member responsible for implementing and monitoring responsible gambling policies within the company.
18. **Self-Assessment Tools** – Online quizzes or surveys that help players identify potential gambling problems and evaluate their gaming habits.
19. **Self-Exclusion** – A voluntary action taken by a player to temporarily or permanently restrict access to gambling services.
20. **Session Monitoring** – A feature that tracks a player's gaming duration, providing real-time updates to encourage responsible play.
21. **Thresholds** – Predefined financial or behavioral limits set by the operator to detect and address excessive gambling activity.
22. **Transaction Blocking** – A security feature that prevents deposits, withdrawals, or wagers from being processed for self-excluded players.
23. **Vulnerable Groups** – Individuals at higher risk of problem gambling, including minors, individuals with gambling addictions, and those with financial or mental health concerns.

1. Introduction

Orakum N.V (hereafter referred to as "Orakum", "Company", "we", or "our") Orakum N.V. is a Curaçao-based company operating in the online gambling industry. It holds a valid Certificate of Operation and has an application (OGL/2024/586/0786) for a gaming license with the Curaçao Gaming Authority. A gaming license issued by the Curaçao Gaming Authority. Orakum N.V under (the registration No. 141651) with its, registered address at Abraham Mendez Chumaceiro Boulevard 03, Curaçao).

Orakum is firmly committed to combating financial crimes, including money laundering, terrorism financing, and proliferation financing. To support this commitment, the company has implemented a robust Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation Financing Policy (AML/CTF/CPF Policy). This comprehensive policy ensures alignment with both national and international regulations and adopts a risk-based approach that spans critical operational domains such as customer interactions, product and service offerings, payment systems, geographic exposure, and service delivery models.

Oversight and enforcement of the AML/CTF/CPF Policy fall under the responsibility of the Board of Directors (BoD) of **Orakum**. The policy is reviewed annually and updated as needed to reflect regulatory changes or shifts in operational risk. Furthermore, a designated compliance officer is empowered to recommend immediate policy updates based on internal or external AML audit outcomes, ensuring timely mitigation of emerging risks.

Orakum adheres strictly to both international standards and the regulatory requirements of Curaçao in relation to anti-money laundering, counter-terrorism financing, and counter-proliferation financing. This compliance is a prerequisite for maintaining its iGaming license under Curaçao jurisdiction. The relevant legal framework includes, but is not limited to:

- **National Ordinance on Identification When Rendering Services (NOIS)** – Articles 2(8) and 11(3)
- **National Ordinance on the Reporting of Unusual Transactions (NORUT)** – Article 22mm(3)
- **Sanctions National Ordinance**
- **Kingdom Sanction Act**

The **Curaçao Gaming Control Board (GCB)** provides a structured regulatory framework that underpins **Orakum**'s internal policies and procedures, aimed at mitigating the risk of financial crime.

The company complies with a broad array of legislative instruments, including:

- NOIS (N.G. 2017, no. 92)
- NORUT (N.G. 2017, no. 99)
- Ministerial Decree on Regulation Indicators Unusual Transactions (N.G. 2015, no. 73)
- Sanctions National Ordinance (N.G. 2014, no. 55)
- Kingdom Sanction Act (N.G. 2016, no. 54)
- National Decree on the Enforcement of the Kingdom Sanction Law (N.G. 2017, no. 2)
- National Decrees implementing UN Security Council Resolutions (N.G. 2015, no. 29, 28)
- National Decree on the Extension of Validity of Sanction Decrees (N.G. 2018, no. 34)

- The Penal Code (N.G. 2011, no. 48)

Together, these statutes and regulations constitute the core legal foundation for AML/CTF/CPF compliance within the Curaçao gaming industry.

In addition to local laws, **Orakum**'s policy incorporates global best practices and aligns with internationally recognized standards, including:

- The **Financial Action Task Force (FATF)** Recommendations
- The **European Union's 4th, 5th, and 6th Anti-Money Laundering Directives (AMLDs)**
- The **Wolfsberg Principles**

By aligning its framework with these global standards, the company ensures a consistent and proactive approach to preventing financial crimes.

Orakum's AML/CTF/CPF Policy has been crafted to meet the compliance expectations of the Curaçao Gaming Control Board. All directors, officers, employees, and third-party compliance auditors are obligated to fully adhere to the policy's principles. Through rigorous enforcement, continuous oversight, and a strong culture of compliance, the company remains steadfast in its mission to provide a secure, transparent, and legally compliant gaming environment.

2. Abbreviations and Definitions

- **AML (Anti-Money Laundering):** A framework of laws, regulations, and procedures established to detect and prevent money laundering and related financial crimes.
- **CTF (Counter-Terrorism Financing):** The process of identifying, preventing, and disrupting financial transactions intended to support terrorist activities.
- **CPF (Counter-Proliferation Financing):** Strategies and controls aimed at stopping the financial support for the proliferation of weapons of mass destruction.
- **KYC (Know Your Customer):** Procedures used to verify a customer's identity and monitor their financial behavior as part of regulatory compliance.
- **CDD (Customer Due Diligence):** A process involving identity verification, risk assessment, and ongoing monitoring of customers to detect potential illicit activity.
- **EDD (Enhanced Due Diligence):** Advanced scrutiny and verification applied to higher-risk customers, entities, or transactions.
- **UBO (Ultimate Beneficial Owner):** The natural person who ultimately owns, controls, or benefits from an account or transaction.
- **SOF/SOW (Source of Funds/Source of Wealth):** The documentation and verification of how a customer's funds or wealth were acquired, to ensure legitimacy.
- **PEP (Politically Exposed Person):** An individual with prominent public functions who presents a higher risk for potential involvement in bribery or corruption.
- **SAR/STR (Suspicious Activity/Transaction Report):** A report submitted to authorities when a transaction or behavior appears suspicious or inconsistent with normal activity.
- **FIU (Financial Intelligence Unit of Curaçao):** The national authority responsible for receiving, analyzing, and disseminating financial intelligence related to suspicious transactions.
- **BoD (Board of Directors):** The governing body of the company tasked with ensuring compliance, corporate governance, and regulatory adherence.
- **Compliance Officer:** A senior official responsible for overseeing AML/CTF/CPF compliance, independent from operational activities.

- **NOOGH (National Ordinance on Offshore Games of Hazard):** Curaçao's primary legislation regulating offshore gaming operations.
- **OFAC (Office of Foreign Assets Control):** A U.S. agency responsible for enforcing economic and trade sanctions.
- **FATF (Financial Action Task Force):** An international body that sets AML/CTF standards and monitors global compliance.
- **CFATF (Caribbean Financial Action Task Force):** A regional group promoting AML/CTF initiatives in the Caribbean and surrounding regions.
- **EU (European Union):** A political and economic union that implements and enforces AML/CTF regulations among its member states.
- **UK (United Kingdom):** A jurisdiction with established AML/CTF frameworks overseen by financial regulatory bodies.
- **US (United States):** A country with robust financial crime oversight through agencies such as OFAC and FinCEN.
- **Risk-Based Approach (RBA):** A strategy for prioritizing AML/CTF efforts based on the relative risk posed by customers, transactions, and jurisdictions.
- **Blacklist:** A register of individuals, entities, or jurisdictions subject to financial restrictions due to AML/CTF concerns.
- **Sanctions:** Legal prohibitions imposed on certain entities or individuals as a result of national security or regulatory violations.
- **Automated Screening Tools (AST):** Software systems that detect high-risk individuals or transactions by screening against global sanctions and watchlists.
- **Economic Sanctions:** Government-imposed restrictions intended to curb illicit financial activity and enforce international law.
- **Curaçao Gaming Control Board (GCB):** The primary regulatory authority for gaming compliance, including AML/CTF measures, in Curaçao.
- **Know Your Business (KYB):** Verification procedures for assessing a business entity's ownership, structure, and financial activities.
- **Structuring:** A money laundering tactic that involves splitting large transactions into smaller amounts to avoid detection.
- **Layering:** A phase in money laundering where funds are moved through complex transactions to obscure their origin.
- **Integration:** The final stage of money laundering in which illicit funds are funneled back into the legitimate economy.
- **Sanctions Evasion:** Attempts to bypass financial restrictions by disguising transactions involving sanctioned parties.
- **First Line of Defense:** Employees who are responsible for collecting KYC data and identifying suspicious activities at the point of customer onboarding or transaction execution.
- **STR (Suspicious Transaction Report):** A formal report documenting transactions that raise AML/CTF concerns, submitted to regulatory bodies.
- **Egmont Group of FIUs:** An international alliance of Financial Intelligence Units that supports global cooperation against financial crime.
- **The Wolfsberg Group:** A collective of global banks that develop AML best practices, particularly in private banking.
- **Audit Logs:** Records kept to demonstrate AML/CTF compliance, required to be stored for a minimum of five years.
- **Reporting Mechanism Audit:** A process that reviews the accuracy and completeness of SARs and related compliance reporting.
- **Unusual Transaction:** A financial activity that deviates from a customer's typical behavior and may indicate suspicious intent.

- **Transaction Monitoring:** The ongoing analysis of financial activity to detect and address potentially illicit transactions.
- **High-Risk Third Country:** A jurisdiction identified by FATF or the EU as having insufficient AML/CTF safeguards.
- **Comprehensive Sanctions:** All-encompassing restrictions that ban all forms of financial engagement with a sanctioned party.
- **Sanctions Compliance and Screening:** Procedures used to prevent financial crime by cross-checking clients and transactions against sanctions lists.
- **Operational Restrictions:** Regulatory actions taken against entities for AML/CTF non-compliance, including penalties or license suspensions.
- **Risk Appetite:** The degree of AML/CTF risk an organization is willing to accept while remaining within its compliance framework.
- **Beneficial Owner:** The individual who ultimately benefits from or controls a legal entity or transaction.
- **Financial Crime Prevention Framework:** A comprehensive system for detecting, preventing, and responding to money laundering and other financial crimes.
- **Customer File Review:** The routine examination of customer records to ensure KYC and CDD standards are being maintained.
- **Senior Management Oversight:** Executive-level responsibility for ensuring the AML/CTF/CPF program is implemented effectively.
- **Training and Awareness Programs:** Educational initiatives that ensure staff understand AML/CTF responsibilities and reporting obligations.
- **Ongoing Monitoring:** Continuous assessment of customer behavior and transactions to identify chnafes in risk.
- **Regulatory Reviews:** Inspections conducted by authorities to confirm the effectiveness and compliance of AML/CTF programs.
- **Corrective Action Plans:** Measures implemented to address and rectify compliance issues identified during audits or regulatory reviews.
- **Periodic Independent Audits:** Third-party evaluations of AML/CTF frameworks to identify weaknesses and improve practices.
- **Internal Control Mechanisms:** Policies and tools designed to protect against financial crime and ensure regulatory compliance.
- **Real-Time Risk Assessment:** The immediate evaluation of transaction risk using automated systems and compliance team input.
- **Confidentiality in Reporting:** The obligation to safeguard sensitive information related to SARs/STRs, ensuring it is not disclosed inappropriately or used to tip off customers.

3. Overview of the iGaming Regulatory Environment

Orakum is a legally incorporated entity in Curaçao. The company holds an active online gaming license (OGL/2024/586/0786) issued by the Curaçao Gaming Control Board, affirming full compliance with jurisdictional regulations and licensing conditions. In accordance with Curaçao's regulatory framework, Orakum is prohibited from offering remote gaming services in certain restricted territories, including the United States, Australia, the Dutch West Indies (Aruba, Bonaire), Curaçao itself, France, Germany, the United Kingdom, Belize, and the Netherlands. Consequently, the company exclusively operates within authorized markets and does not engage with users in jurisdictions where online gaming is legally prohibited.

Like other online gaming and betting platforms, Orakum faces inherent financial crime risks such as identity fraud, money laundering, structuring, layering, and internal or external collusion. To address these risks, the company has implemented a comprehensive Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation Financing (AML/CTF/CPF) compliance framework. This includes stringent security measures and due diligence protocols aimed at detecting and preventing illicit financial activity within its ecosystem.

4. Money Laundering, Terrorism Financing & Proliferation Financing

Money Laundering

Money laundering is a critical enabler of financial crimes, often involving complex international transactions. It supports various forms of criminal behavior, including tax evasion, bribery, corruption, sanctions breaches, drug and arms trafficking, extortion, and kidnapping. The principal objective is to disguise the illicit origin of funds, concealing their true source, ownership, and intended use.

The Three Stages of Money Laundering:

- **Placement:** Illicit funds are introduced into the financial system through activities such as bank deposits, asset purchases, or monetary transfers.
- **Layering:** Funds are moved through multiple financial channels to obscure their origin—this includes currency conversions, transfers across accounts, and the purchase of financial instruments.
- **Integration:** The ‘cleaned’ funds are reintegrated into the legitimate economy, often through real estate, luxury goods, or business investments.

Online gambling platforms are particularly susceptible to laundering due to their high transaction volumes and potential anonymity. This underscores the necessity for robust monitoring systems to flag irregularities and prevent abuse.

Terrorism Financing

Terrorism financing involves the provision or collection of funds to support terrorist operations, regardless of whether the funds originate from legal or illegal sources. Unlike traditional money laundering, these funds may be legally obtained but are repurposed for unlawful ends.

Sources of Terrorist Financing:

- **Legitimate Channels:** Businesses, donations, and charities may be exploited to covertly funnel money to terrorist causes.
- **Illicit Means:** Criminal activities such as smuggling, fraud, and narcotics trade serve as primary revenue streams for terrorist entities.

Common Transfer Methods:

- **Formal Banking Systems:** Used to structure and layer funds below reporting thresholds.
- **Informal Networks:** Systems such as hawala are leveraged to move money outside traditional oversight mechanisms.

Red Flags for Terrorist Financing:

- Transactions inconsistent with known customer profiles.
- High-frequency or high-value transfers to or from high-risk regions.
- Dealings with individuals or organizations listed on international sanctions databases.
- Use of large cash deposits or businesses in high-risk sectors.

To combat these threats, **Orakum** (Reg. Number: 141651) has developed a robust AML/CTF compliance structure that includes:

- Enhanced due diligence on high-risk customers.
- Continuous transaction monitoring for red flags.
- Timely reporting of suspicious transactions to the relevant regulatory bodies.

Orakum strictly follows key regulatory frameworks, including:

- **Sanctions National Ordinance (SNO, N.G. 2014, no. 55)**
- **Kingdom Sanction Act (N.G. 2016, no. 54)**
- **Curaçao Gaming Control Board (GCB) guidelines**
- **OFAC, EU, UN, and U.S. terrorism-related sanctions and watchlists**

These efforts align with global counter-terrorism financing standards, including those from:

- **Financial Action Task Force (FATF)**
- **Office of Foreign Assets Control (OFAC)**
- **European Union Regulations**
- **United Nations Sanctions**

Through these mechanisms, **Orakum** ensures it does not inadvertently facilitate or support terrorist activities through its operations.

Proliferation Financing

Proliferation financing pertains to the provision or movement of funds and resources used in the development, acquisition, or dissemination of weapons of mass destruction (WMDs). This form of financing poses significant global risks and is explicitly prohibited by international laws and Curaçao's legal standards.

As a licensed gaming operator, **Orakum** actively works to identify and prevent the misuse of its platform for such purposes. This is achieved through its broader AML/CTF/CPF compliance program, which includes the following:

1. Compliance with Regulatory Standards:

The Curaçao Gaming Control Board mandates that all iGaming operators, including Orakum, implement measures to prevent proliferation financing. Orakum adheres to these regulations and incorporates global best practices.

2. Proliferation Risk Assessments:

Regular assessments are conducted to detect risks associated with high-risk jurisdictions and transactions involving entities or items that may be linked to WMD proliferation.

3. Enhanced Due Diligence (EDD):

High-risk customers and transactions are subjected to rigorous scrutiny, including:

- Screening against international sanctions lists (UN, FATF, EU).
- Investigation of anomalies in transaction behavior.
- Monitoring for links to flagged organizations.

4. Transaction Monitoring & SAR Filing:

Advanced monitoring tools are used to detect suspicious financial behavior. Suspected proliferation-related transactions are escalated to compliance officers and reported to the **Curaçao Financial Intelligence Unit (FIU)** when warranted.

5. Sanctions Screening & Record-Keeping:

The company conducts comprehensive sanctions screenings and maintains detailed records of all compliance activities, ensuring transparency and audit-readiness.

6. Employee Training & Awareness:

Staff receive regular, specialized training focused on proliferation financing threats and red flags. This ensures personnel are equipped to identify risks and respond appropriately.

7. Regulatory Cooperation:

Orakum collaborates with the GCB, FIU, and other enforcement agencies by sharing intelligence, submitting reports, and participating in industry-wide initiatives to strengthen financial crime defenses.

8. Commitment to Global Security:

By implementing proactive measures and adhering to national and international obligations, **Orakum** reinforces its role as a secure, responsible participant in the financial and iGaming sectors, supporting broader efforts to disrupt illicit financial networks connected to WMDs.

5. Sanctions Adherence and Compliance Framework

Orakum (Reg. Number: 141651) is fully committed to complying with international sanctions laws as an integral part of its broader Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) framework. The company maintains a rigorous sanctions compliance program designed to prevent any financial interactions with sanctioned individuals, organizations, or jurisdictions. All customers and transactions are subject to thorough due diligence and real-time screening processes to ensure full adherence to regulatory requirements and to minimize the risk of sanctions violations.

Transaction Monitoring and Regulatory Reporting

A core element of Orakum's compliance strategy is the continuous monitoring of financial transactions. Sophisticated, automated screening systems operate in real time, scanning all transaction activity for potential links to sanctioned parties. Any anomalies or red flags are immediately escalated for review by the compliance team. Where necessary, such activities are reported to the relevant authorities in accordance with applicable regulations.

To further support sanctions compliance, Orakum conducts ongoing training programs for its employees. These programs ensure that staff remain up to date on evolving sanctions regimes, enforcement practices, and compliance obligations, enabling them to identify and respond to potential violations effectively.

Automated Sanctions Screening and Response Protocols

To maintain full compliance, Orakum employs automated sanctions screening tools across all user interactions and financial operations. These systems are integrated with up-to-date global sanctions databases, enabling the company to detect potential compliance breaches swiftly and accurately. The sanctions lists are regularly updated to reflect the latest additions from national and international regulatory bodies.

If a potential match is identified, Orakum promptly takes appropriate action—such as freezing accounts, halting transactions, and initiating enhanced investigations. Verified sanctions breaches are immediately reported to the appropriate authorities, reflecting the company's zero-tolerance policy toward non-compliance.

6. Risk-Based Compliance Framework

A core pillar of **Orakum's** compliance framework is its structured risk assessment process, built around a **risk-based approach (RBA)**. This approach involves systematically evaluating risks related to customer profiles, products, services, transaction types, and geographic exposure. The goal is to proactively identify and address potential vulnerabilities before they can impact operations. Through ongoing assessments, Orakum enhances its ability to detect, assess, and respond to emerging financial crime threats while maintaining full alignment with Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) obligations.

Implementation of Risk Mitigation Controls

Once risks are identified, **Orakum** applies tailored mitigation strategies based on the level and type of risk exposure. These strategies form the foundation of its financial crime prevention efforts, enabling the company to counter threats such as money laundering, terrorism financing, and proliferation financing.

A key component is **Enhanced Due Diligence (EDD)**—a more rigorous review process for high-risk customers and transactions. This includes detailed assessments of the source of funds, verification of beneficial ownership structures, and scrutiny of financial histories. These procedures are essential in detecting hidden financial risks and blocking illicit financial flows.

Orakum also deploys real-time **transaction monitoring systems**, which use automated alerts to flag suspicious activity patterns—such as sudden large deposits or unusual transfer behaviors. Custom alert thresholds enable swift reviews and investigations of potentially illicit activities.

Customer verification is further reinforced through robust identity checks, especially for high-risk clients. This includes verification against trusted data sources and continuous monitoring for red flags.

These steps ensure only verified individuals can engage in financial transactions on the platform.

Ongoing Monitoring and Policy Adaptation

To stay aligned with dynamic regulatory environments, **Orakum** regularly reviews customer behavior, transaction trends, and risk indicators. This **continuous monitoring** allows for real-time detection of emerging risks, reclassification of customer risk levels, and timely updates to AML/CTF/CPF policies. The adaptability of this compliance framework enables Orakum to maintain effectiveness amid changing threat landscapes.

Accurate Reporting and Record Maintenance

A critical aspect of Orakum's RBA framework is its commitment to **accurate reporting and meticulous record-keeping**. Suspicious transactions are reported to the appropriate authorities without delay, following legal requirements. Comprehensive records of identity verification, financial activity, and risk assessments are retained for the mandatory duration and are readily available for audit or regulatory inspection—demonstrating Orakum's dedication to transparency and legal integrity.

Commitment to a Secure, Compliant Environment

Through the strategic implementation of risk assessments, tailored mitigation tactics, and regulatory vigilance, **Orakum** ensures a secure, fully compliant gaming environment. Ongoing enhancements to monitoring systems and employee training programs reinforce its commitment to preventing financial crime and maintaining trust with regulators, partners, and users alike.

6.1 Risk Factors

Customer Risk and Risk-Based Assessments

Customer risk represents the likelihood of exposure to money laundering (ML) and terrorist financing (TF) stemming from interactions with specific individuals. As part of its risk-based compliance model, **Orakum** evaluates customer profiles based on identity, financial behavior, source of wealth, and transaction history to identify and manage potential vulnerabilities.

Certain customer segments are inherently riskier. These include individuals with multiple or unverifiable income sources, those with inconsistent financial patterns, and **Politically Exposed Persons (PEPs)**—who, due to their public positions and access to state funds, are subject to elevated scrutiny for corruption and abuse of power.

Additional high-risk profiles may include:

- **High spenders** whose financial activity exceeds their declared income;
- **Disproportionate spenders** engaging in transactions beyond reasonable financial means;
- **Customers using multiple accounts**, who may attempt to disguise betting behavior or evade detection.

To address these risks, **Orakum** has established transaction thresholds aligned with expected customer behavior. While low-risk individuals typically have a single, verifiable income

source, higher-risk customers are subject to enhanced due diligence (EDD) and ongoing transaction monitoring.

Product, Service, and Transaction Risks

Certain gaming offerings and transaction types present a greater risk of exploitation for ML/TF. Criminal organizations may exploit vulnerabilities within gaming ecosystems to conceal the origin of illicit funds.

Common risks include:

- **Use of criminal proceeds** from activities like fraud, trafficking, or theft deposited into gaming accounts;
- **Anonymous payment methods**, such as prepaid cards or cryptocurrencies, which offer limited traceability;
- **Gaming accounts used solely for deposits/withdrawals**, without genuine gaming activity;
- **Peer-to-peer transfers**, enabling covert fund movement between users;
- **Use of third-party financial tools**, such as bank accounts or cards not registered to the customer;
- **Cross-platform fund transfers**, which make tracking more complex;
- **Multi-operator gaming networks**, allowing users to circumvent controls through layered accounts.

To mitigate these risks, **Orakum** conducts ongoing transaction monitoring, applies EDD measures where needed, and ensures strict compliance with global AML/CTF/CPF standards.

Geographical Risk

Geographical risk refers to threats associated with the locations of customers or the origin of their funds, particularly from jurisdictions with poor AML/CTF oversight, high corruption levels, or active sanctions.

High-risk regions are monitored using trusted sources such as:

- **FATF high-risk and monitored jurisdictions;**
- **CFATF regional advisories;**
- **U.S. Department of State INCSR reports;**
- **EU lists of high-risk third countries;**
- **OFAC sanctions and enforcement actions;**
- **Transparency International's Corruption Perceptions Index (CPI).**

Orakum utilizes a country classification model to distinguish high- and low-risk jurisdictions. Customers from high-risk regions are subject to EDD, stricter onboarding processes, and heightened transaction monitoring. Transactions involving sanctioned countries are blocked, and monitoring protocols are regularly updated to reflect the latest geopolitical developments and compliance risks.

Distribution Channel Risks and Controls

The manner in which **Orakum** delivers its services can also pose financial crime risks—especially through channels that allow for anonymity or reduced oversight.

To counter these risks, the company enforces:

- **Stringent verification for non-face-to-face transactions;**
- **Biometric and multi-factor authentication technologies;**
- **Advanced identity verification systems** to ensure genuine user interaction.

These efforts help prevent fraud, detect high-risk behaviors early, and support compliance with international regulatory standards, ensuring that all customer engagement channels remain secure and transparent.

6.2 Technological Developments Risk Assessment

As the iGaming sector rapidly evolves through technological innovation, **Orakum** is committed to ensuring that new digital capabilities do not create opportunities for financial crime. The company has embedded a proactive **technological risk assessment process** into its compliance framework to identify and mitigate risks linked to new products, services, and operational technologies.

Technology-Driven Risk Identification

Orakum conducts comprehensive evaluations whenever:

- A **new product** or **feature** is launched;
- A **business process** is updated or automated;
- A new **payment method** or **digital platform** is introduced;
- Advanced technologies—such as **blockchain**, **AI**, or **automated services**—are adopted.

Each innovation undergoes a full compliance risk assessment to determine whether it could be misused for illicit purposes. Findings are documented, and control measures are applied in line with both Curaçao's legal requirements and international AML/CTF expectations.

Implementation of Technological Safeguards

When potential risks are identified, **Orakum** takes immediate action through:

- **Enhanced security infrastructure**, including biometric verification, encryption, and AI-powered fraud detection;
- **Upgraded transaction monitoring systems** capable of identifying suspicious patterns tied to new technologies;
- **Policy updates** to reflect emerging digital risks and evolving criminal methodologies.

This ensures the company remains compliant, secure, and adaptive to changes in the tech landscape.

By continuously assessing technological risk, refining controls, and adapting policies, **Orakum** preserves the integrity of its operations while maintaining full compliance with AML/CTF/CPF obligations. This forward-looking approach ensures that innovation and security evolve together, enabling the company to remain both competitive and compliant in a rapidly transforming industry.

7. Due Diligence

Orakum (Reg. Number: 141651) is firmly committed to regulatory compliance and the prevention of anonymous or fraudulent accounts. As part of its Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) framework, the company enforces strict identity verification procedures to ensure all business relationships with players are legitimate.

Through the implementation of comprehensive Customer Due Diligence (CDD) protocols, **Orakum** is equipped to identify and mitigate risks associated with financial crime, including money laundering, terrorism financing, and proliferation financing. All suspicious activity uncovered during the due diligence process is reported to the Financial Intelligence Unit (FIU), with serious cases escalated to the Public Prosecutor's Office when appropriate. These proactive measures reflect Orakum's commitment to regulatory adherence and responsible gaming.

7.1. Comprehensive Customer Due Diligence Measures

Player Identification and Verification

As part of its CDD program, **Orakum** applies a rigorous identity verification process that includes:

- Validation of identity through trusted, independent sources (e.g., government-issued ID).
- Identification of Ultimate Beneficial Owners (UBOs) for corporate entities.
- Understanding the nature and purpose of the business relationship.
- Continuous monitoring to ensure financial activity aligns with customer risk profiles and declared source of funds.

Confidential Reporting Procedures

To prevent tipping off customers, Orakum employees are strictly prohibited from disclosing when a Suspicious Activity Report (SAR) has been filed with the FIU. If standard CDD procedures might reveal that an investigation is underway, the company may bypass certain steps and report the activity immediately.

7.2. Player Identity Verification Process

Required Information

Players must provide:

- Full legal name
- Date and place of birth
- Residential address
- Nationality
- Official ID number (passport, ID card, or driver's license)

For low-risk individuals, this basic data may suffice. High-risk individuals are subject to additional verification measures.

Risk Assessment and Validation

Upon registration, each player undergoes a risk assessment, updated continuously as new data becomes available. Verification includes:

- Review of photo ID
- Address confirmation through recent documents
- Biometric checks and database cross-matching
- IP tracking and source of funds analysis

If initial data is insufficient, Orakum may require:

- A live selfie with identification
- Verification of the first deposit from a regulated institution

7.3. Understanding the Business Relationship

Orakum seeks to understand the nature of each customer relationship. While the primary purpose is clear—online gaming—the company gathers data to detect unusual or suspicious activity.

For high-risk customers, **Enhanced Due Diligence (EDD)** includes:

- Documentation of source of wealth
- Analysis of financial and gaming behavior
- Cross-checks against third-party databases

Low- and medium-risk customers may provide:

- A basic employment or income declaration
- Additional information only if anomalies are detected

This tiered approach ensures proportional due diligence while meeting compliance obligations.

7.4. Ongoing Monitoring and Compliance Oversight

Orakum continuously monitors players and their transactions as part of its AML/CTF/CPF program.

Key actions include:

- Regular updates to player information, especially for high-risk accounts
- Transaction monitoring to detect suspicious patterns
- EDD applied to transactions equal to or exceeding NAF 4,000 (including linked transactions)
- Real-time risk alerts and investigation of flagged activities

Suspicious transactions are escalated and, where necessary, reported to the FIU. By combining automated detection with expert review, Orakum maintains a secure and compliant platform.

7.5. Simplified and Enhanced Due Diligence

Simplified Due Diligence (SDD)

SDD may be applied where the risk of ML/TF is minimal. Measures include:

- Collecting only basic personal details
- Delayed verification after account setup (where legally permissible)
- Reduced frequency of updates and lower-intensity transaction monitoring

SDD cannot be used if:

- Suspicious activity is detected
- The customer is high-risk

Enhanced Due Diligence (EDD)

EDD applies to customers presenting higher financial crime risks. Triggers include:

- Residence in high-risk jurisdictions
- PEP status
- Use of anonymous financial instruments (e.g., crypto, prepaid cards)
- Involvement in emerging financial technologies

EDD measures include:

- Collection of additional personal and financial data
- Detailed source of funds verification
- Transaction monitoring with automated alerts
- Senior management approval for high-risk relationships
- Verification of the first deposit from a regulated source

7.6. Timing of Due Diligence Procedures

Orakum applies CDD promptly, in accordance with regulatory thresholds.

Threshold-Based Verification

Customer identity is verified when:

- A single or cumulative transaction equals or exceeds NAF 4,000
- The customer reaches the threshold via deposit, withdrawal, or peer-to-peer activity

Before reaching this threshold, Orakum proactively verifies customer identities during registration to prevent misuse.

Restrictions While CDD is Pending

If the NAF 4,000 threshold is met and verification is incomplete:

- Further deposits/withdrawals are restricted
- Accounts may be frozen pending verification

If documents are not provided within 30 days:

- The business relationship is terminated
- Funds are returned to the original payment method (unless ML/TF is suspected, in which case they may be blocked)
- FIU is notified if suspicion of financial crime exists

Avoiding Tipping Off

Each case is handled carefully to avoid alerting customers to ongoing investigations, while ensuring compliance with AML/CTF laws.

7.7. Due Diligence for Existing Clients

CDD is not limited to new customers. Orakum monitors and reassesses existing clients on an ongoing basis to maintain compliance.

When re-verification is required:

- If a customer's risk profile changes (e.g., new jurisdiction, PEP designation)
- Following regulatory changes or legal triggers
- Upon reaching the NAF 4,000 transaction threshold

If past CDD was incomplete, Orakum prioritizes retrospective verification for high-risk clients, ensuring consistent compliance across all customer relationships.

7.8. Termination of Customer Relationships

Orakum terminates business relationships when:

- A player fails to comply with CDD requirements
- Suspicious financial activity is identified
- The customer is assessed as high-risk for ML/TF

Termination involves:

- Review and approval by senior management
- Final assessment of account history
- Reporting any red flags to the FIU
- Retention of records for a minimum of five years

This strict enforcement policy upholds the platform's security and compliance integrity.

7.9. Third-Party Reliance in CDD Processes

Orakum may utilize third-party services to carry out specific elements of the CDD process; however, it retains full responsibility for compliance.

Safeguards include:

- Immediate access to all customer identification data
- Written agreements outlining the third party's obligations
- Engagement only with regulated entities subject to AML/CFT supervision
- Independent risk assessments of the third party's jurisdiction

Third-party reliance differs from outsourcing:

- **Reliance** involves using independently gathered CDD data, with Orakum accountable for compliance.
- **Outsourcing** means the third party applies Orakum's internal CDD procedures under direct oversight.

All arrangements are subject to periodic review and audit to ensure regulatory standards are upheld.

8. Suspicious Activity Reporting

Orakum (Reg. Number: 141651) is fully committed to the timely identification and reporting of any activities that may be associated with money laundering (ML) or terrorist financing (TF). Indicators of such risks may include unusual client behavior, large or unexplained financial movements, or transactions involving high-risk jurisdictions. All employees are required to remain vigilant and report any concerns immediately to the appointed Compliance Officer.

Upon receiving a report, the Compliance Officer will conduct a detailed review to determine whether internal controls should be activated and whether the activity warrants formal reporting to relevant authorities, including the Financial Intelligence Unit (FIU).

Identifying Unusual Transactions

Transactions that deviate significantly from a customer's normal behavior or financial activity are classified as unusual. These may include:

- Large, uncharacteristic transfers of funds
- Dealings with unverified or unfamiliar third parties
- Transactions lacking a clear legal, economic, or legitimate purpose

Staff rely on automated monitoring tools and their training to flag such transactions, which are then forwarded to the Compliance Officer for further evaluation.

Transaction Types Subject to Reporting

In accordance with applicable regulations, **Orakum** considers the following types of transactions to be potentially suspicious and subject to further scrutiny:

1. Transactions Previously Flagged for ML/TF

Any transaction that has already been reported to law enforcement, the judiciary, or other authorities as potentially linked to ML or TF must automatically be treated as unusual.

2. Dealings Involving Sanctioned Individuals or Entities

Transactions involving persons or organizations listed under the **Sanctions National Ordinance (N.G. 2014 no. 55)**, or other applicable sanctions frameworks, are treated as suspicious and reviewed accordingly.

3. Transactions Equal to or Above NAF 5,000

Any financial activity—regardless of payment method—that meets or exceeds the NAF 5,000 threshold must be flagged. This includes:

- **Cash transactions:** Deposits or withdrawals at or above the threshold
- **Gaming-related purchases:** Acquisition of chips, tokens, or digital credits totaling NAF 5,000 or more
- **Payouts:** Redemption of winnings or other cash disbursements reaching or exceeding the same amount

This rule applies to both individual transactions and cumulative daily activity. Multiple transactions that collectively surpass NAF 5,000 within a single day must be assessed in totality.

If there is any reasonable suspicion—based on transaction behavior, customer profile, or contextual red flags—that the activity may relate to ML or TF, it must be treated as a **presumptively suspicious transaction** and escalated without delay.

Confidentiality in Reporting

To preserve the integrity of the suspicious activity reporting process and comply with legal obligations, **strict confidentiality** is maintained regarding all Suspicious Activity Reports (SARs). Employees must not inform the customer or any unauthorized third party about the filing of a SAR. This prohibition is essential to avoid **tipping off**, interfering with investigations, or compromising enforcement efforts.

Only authorized personnel—such as the Compliance Officer and designated members of the compliance team—are permitted access to SAR-related information. Staff are trained on the importance of discretion and the legal implications of confidentiality breaches.

Any violation of the confidentiality policy is treated as a serious compliance infraction and may result in disciplinary action, including termination. These measures ensure that Orakum's AML/CTF/CPF framework remains effective, secure, and fully aligned with legal and regulatory expectations.

By fostering a culture of awareness, accountability, and discretion, **Orakum** reinforces its dedication to regulatory compliance and strengthens its capacity to detect and report suspicious activities. This commitment supports broader efforts to combat financial crime and uphold the integrity of the iGaming sector.

9. Designated Compliance Officer

The **Compliance Officer** plays a vital role in safeguarding **Orakum** (Reg. Number: 141651) against risks related to money laundering (ML), terrorism financing (TF), and proliferation financing (PF). As the central authority within the company's AML/CTF compliance structure, the Compliance Officer is responsible for the design, implementation, and oversight of all anti-financial crime measures in accordance with Curaçao's legal framework and international regulatory standards.

A primary responsibility of the Compliance Officer is the development and continuous enhancement of the AML/CTF/CPF compliance program. This includes:

- Drafting and updating internal policies
- Ensuring alignment with national and international regulations
- Conducting regular evaluations to measure the effectiveness of compliance controls
- Advising senior leadership on regulatory developments and risk mitigation strategies

To foster a culture of compliance, the Compliance Officer organizes ongoing training programs for all employees. These sessions focus on emerging financial crime threats, regulatory updates, and practical guidance for recognizing and reporting suspicious activity.

In addition to policy management and training, the Compliance Officer oversees transaction monitoring and internal investigations. They are responsible for:

- Reviewing unusual financial activities
- Assessing transactions under the Ministerial Decree on Unusual Transactions
- Filing Suspicious Activity Reports (SARs) with the Financial Intelligence Unit (FIU)
- Deciding when account freezing or blocking is required to comply with anti-tipping-off laws

The Compliance Officer remains proactive in identifying regulatory risks and strengthening the AML/CTF/CPF framework. This includes:

- Monitoring global developments in financial crime prevention
- Recommending process improvements
- Providing management with periodic compliance reports summarizing risk findings, audit outcomes, and implementation progress

Through diligent oversight, training, and continuous refinement of compliance measures, the Compliance Officer ensures **Orakum** upholds a high standard of legal and regulatory integrity within the iGaming industry.

10. Independent Audit

To ensure full compliance with Curaçao's updated iGaming regulations, **Orakum** (Reg. Number: 141651) undergoes periodic **independent audits** of its Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) programs. These audits assess the effectiveness of the company's financial crime controls, identify areas for improvement, and verify alignment with both domestic and international regulatory expectations. The audit process is overseen by the **Curaçao Gaming Control Board (GCB)**.

Objective and Scope

The main objective of the AML/CTF/CPF audit is to evaluate the robustness of Orakum's compliance framework. Regular audits enable the company to:

- Proactively identify weaknesses or gaps
- Strengthen internal risk controls
- Benchmark its program against industry best practices
- Demonstrate continued regulatory compliance

Audit reviews cover a broad range of compliance areas, including:

- Risk assessments
- Transaction monitoring systems
- Employee training programs
- Customer due diligence procedures
- Reporting and escalation protocols

Engagement of an Independent Auditor

To maintain impartiality, **Orakum** engages an external independent auditor—or in certain cases, a specialized internal team separate from the compliance function. The auditor’s qualifications, expertise in AML/CTF/CPF regulations, and independence are evaluated and approved by the **Curaçao Gaming Control Board** prior to engagement.

Audit Components

Audits follow international compliance standards and GCB-issued guidelines, and include:

- **Policy & Procedure Review** – Evaluates whether AML/CTF/CPF policies are current, effective, and properly implemented
- **Risk Management Review** – Assesses the methodology for identifying and managing high-risk transactions, clients, and jurisdictions
- **Monitoring & Reporting** – Verifies that systems detect and report suspicious transactions accurately and in compliance with SAR obligations
- **Employee Training Review** – Assesses whether staff receive appropriate training on risk indicators, escalation procedures, and legal responsibilities
- **Customer Due Diligence Review** – Audits customer records for adherence to KYC, KYB, and CDD requirements
- **Reporting Mechanism Audit** – Reviews SAR filing procedures to ensure legal and procedural accuracy

Audit Findings and Follow-Up

Following the audit, the auditor prepares a comprehensive report summarizing findings, recommendations, and any identified deficiencies. This report is submitted to Orakum’s senior management and the **Curaçao Gaming Control Board**.

In response, **Orakum**:

- Implements corrective actions within defined timelines
- Updates internal processes to close compliance gaps
- May be subject to follow-up audits to validate improvements

Regulatory Oversight by the Gaming Control Board

The GCB actively monitors licensed operators for compliance and may:

- Review submitted audit reports
- Request additional documentation
- Conduct site visits or interviews with senior management and the Compliance Officer
- Evaluate the implementation of audit recommendations

Consequences of Non-Compliance

Failure to meet AML/CTF/CPF obligations may result in:

- Monetary fines
- Temporary operational restrictions

- Suspension or revocation of the gaming license in cases of serious or repeated breaches

To mitigate these risks, **Orakum** maintains continuous communication with the GCB and takes a proactive approach to meeting all regulatory expectations.

Commitment to Compliance

By conducting regular, independent AML/CTF/CPF audits and ensuring full regulatory cooperation, **Orakum** demonstrates its ongoing commitment to financial crime prevention, operational transparency, and regulatory excellence. These audits form a critical part of the company's compliance strategy, helping maintain integrity and trust in its operations within the global iGaming ecosystem.

11. Management Responsibilities

At **Orakum**, strong governance begins at the top. The company's senior management and Board of Directors play a vital role in safeguarding the business from financial crime risks by actively overseeing all Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) efforts.

Management oversight is more than a regulatory obligation—it's a core part of Orakum's culture. The appointed AML/CTF/CPF Compliance Officer provides the Board with regular reports detailing changes in risk exposure, evolving regulatory requirements, and updates to the compliance framework. An annual effectiveness assessment ensures these safeguards remain robust, responsive, and aligned with global best practices.

To ensure policies stay current and effective, management conducts an annual policy review informed by monthly risk assessments. If vulnerabilities are identified, the Compliance Officer presents actionable recommendations to the Board for swift implementation. This ongoing review process reinforces Orakum's commitment to continuous improvement and regulatory excellence.

Training is another cornerstone of management responsibility. Orakum ensures all staff—especially those in sensitive or high-risk roles—receive relevant, ongoing compliance training. These programs empower employees to recognize red flags and respond to suspicious activity, fostering a company-wide culture of awareness and accountability.

Senior management also ensures strong internal controls through proper role segregation, clearly defined authorization protocols, and constant oversight. Documentation is meticulously maintained, ensuring transparency across all financial operations. In addition, independent audits are conducted regularly to evaluate and strengthen Orakum's AML/CTF/CPF framework—providing objective insights and helping the company stay ahead of compliance expectations.

12. Training & Record Keeping

Employee Training

At **Orakum**, knowledge is the first line of defense against financial crime. That's why the company has built a comprehensive AML/CTF/CPF training program to ensure every employee is equipped to detect and prevent suspicious activities.

Training is tailored to each role, with mandatory participation for all team members—from frontline support staff to senior executives. Whether monitoring transactions, verifying customer identities, or managing compliance reports, employees receive specialized instruction aligned with their responsibilities.

New hires undergo a full onboarding program that introduces them to Orakum's compliance obligations, internal procedures, and reporting expectations. All employees participate in mandatory refresher courses at least once per year, while those in high-risk roles—such as compliance officers and customer verification teams—receive additional, frequent training to stay ahead of emerging threats.

The curriculum covers a wide range of topics, including:

- Curaçao AML/CTF/CPF legislation
- Internal policies and compliance procedures
- Know Your Customer (KYC) and Customer Due Diligence (CDD) protocols
- Identification of suspicious transactions and red flag behaviors
- Record-keeping and reporting obligations
- Sanctions awareness and high-risk jurisdiction screening

Training sessions are delivered through engaging formats like workshops, webinars, e-learning modules, simulations, and real-life case studies. This hands-on approach ensures not just knowledge—but practical application.

Led by qualified internal experts and external consultants, the training content is continuously updated to reflect regulatory changes and global compliance trends. By investing in its people, **Orakum** builds a resilient, compliance-aware workforce that upholds the highest standards of integrity.

Record Keeping

Effective compliance depends on more than just knowing the rules—it requires impeccable documentation. At **Orakum**, record keeping is a top priority, forming the backbone of the company's AML/CTF/CPF compliance strategy.

The company maintains detailed records of:

- Customer identification and verification
- Transaction histories
- Suspicious Activity Reports (SARs)
- Training completion logs
- Internal audits and compliance assessments

In accordance with Curaçao's regulatory requirements, these records are retained for a minimum of **five years** and are readily accessible during audits or investigations.

Security is at the core of Orakum's record-keeping system. All data is encrypted and protected with strict access controls. Only authorized personnel have access, and every interaction is logged to ensure full accountability. Regular internal and external audits are conducted to verify data integrity and detect any vulnerabilities.

Orakum also uses a structured classification and retrieval system to ensure fast and accurate access to documentation when required. This efficiency supports both day-to-day operations and regulatory inquiries, reinforcing the company's reputation for transparency and compliance readiness.

By maintaining well-organized, secure, and auditable records, **Orakum** ensures full compliance with AML/CTF/CPF obligations while demonstrating its commitment to ethical, accountable business practices.