

Business Plan for Curaçao Licensing and Compliance Services (CLCS)

Date: July 2025

Location: Willemstad, Curaçao

Website: www.clcs.io

Email: info@clcs.io



Executive Summary

In **2024**, Curaçao passed its gambling regulations through the **National Ordinance for Games of Chance (LOK)**, aiming to align more closely with international standards (e.g., UKGC, MGA). These reforms emphasize:

- Player protection.
- Transparency in dispute resolution.
- Responsible gambling measures.

Operators preparing for future licensing under the LOK framework would **benefit from externalizing key compliance areas** like complaint resolution and self-exclusion. **Curaçao Licensing Compliance Services (CLCS)** is a compliance and technical support firm based in Curaçao, focused on delivering high-integrity, tech-enabled services for online gaming and iGaming operators. Our flagship product, the **Live Heartbeat Seal**, offers real-time assurance of operational compliance and player safety, adding transparency and trust to any licensed platform. CLCS' team has more than 10 years handling several types of ADR cases and has more than 25 years' experience in the online gaming industry on several levels.

CLCS supports operators through a suite of services designed to satisfy Curaçao's evolving regulatory environment and international best practices. Services include **Alternative Dispute Resolution (ADR)**, **self-exclusion systems**, and **digital record-keeping (Player's data back up service)**, for operational privacy and flexibility according to requirements by the new Curaçao Gaming Law. All services under 1 compliance seal.

GCB or GCA do not handle individual complaints against gaming providers. Resolving disputes between players and gaming operators is not within our mandate. As such, GCB, nor GCA do not have the authority to mediate or arbitrate in these matters. Here is where CLCS comes in to assist each operator.

Vision & Mission

Vision:

To be the leading compliance partner for iGaming operators in Curaçao, redefining trust and accountability in the digital gaming industry and adhering by the current gaming law.

Mission:

To offer transparent, efficient, and technologically advanced compliance and dispute resolution services that empower licensed operators and protect players.

Advantages of Third-Party Handling: Complaints & Self-Exclusion

1. Increased Trust and Transparency

- **Players perceive impartiality** when complaints and self-exclusion are handled by an independent body, improving trust in the operator.
- Helps reduce suspicion of bias or internal conflicts of interest.

2. Regulatory Compliance

- Curaçao's laws, **recent reforms (especially post-2024)** are moving towards stricter compliance.
- Using a third party demonstrates proactive **responsible gambling practices** and can help meet evolving **regulatory expectations**, including:
 - Fair complaint resolution.
 - Enforced self-exclusion across platforms or operators.

3. Risk Mitigation

- Reduces legal and reputational risks if complaints are mishandled.
- Limits potential for **regulatory penalties**, fines, or license issues.

4. Better Record-Keeping and Reporting

- Third parties typically maintain logs of all complaints and exclusion actions, which can support audits and compliance checks.
- Easier to provide documentation to regulators when requested.

5. Operational Efficiency

- Frees up internal resources; instead of dedicating staff to handle complaints and exclusions, operators can focus on core business operations.
- Third-party services may offer **faster response times** and **better case management systems**.

6. Improved Responsible Gaming Outcomes

- External services may provide better tools or frameworks for monitoring problematic behavior.
- More effective **self-exclusion enforcement**, particularly if the provider operates across multiple platforms or integrates with central exclusion registers.

Services Overview

1. Live Heartbeat Seal (Flagship Product)

A real-time digital badge embedded into operators' websites indicating current compliance status. Features include:

- Verification of license status
- Providing Alternative Dispute Resolution to players
- Integrated links to self-exclusion tools
- Offer player's data back up services to Tier IV Data Center in Curaçao

2. ADR Services – Complaints Handling & Dispute Resolution

ADR (Alternative Dispute Resolution) is a process that allows consumers (players) to resolve disputes with a business (gaming operator) without going to court. It's especially critical in regulated sectors like online gambling.

- Neutral mediation between players and operators
- Handle the dispute according to template provided by CGA
- Adhere by the process and time frame stipulated in the LOK
- Custom-built dispute ticketing system
- Outcomes published (where appropriate) for transparency
- Certified mediators and internal compliance experts

CLCS offers different types of players complaint (ADRs) services, but not limited to:

- Wagering disputes (Sports, Casino, Poker) – including LIVE Dealer disputes
- Bonus disputes (Promotional terms, bonus abuse etc.)
- Probability disputes (Random Number Generator – RNG)
- Deposit/Withdrawal disputes (FIAT & Crypto)
- Responsible Gaming disputes
- Problem Gambling disputes – including self-exclusion)
- Legal threats / demand letters
- Underage cases
- Jurisdictional cases
- ATOs (account take overs – players claiming others have accessed their account)
- Alleged “unfair” treatment towards the player by CS/management
- Seizure or voiding of funds (often due to fraudulent activity in the account)
- Player Verification/Identity disputes
- Fraud Case disputes involving;
 - Stolen identity
 - Multi-accounting
 - Non-recreational gameplay (often in relation to referral abuse)
 - System vulnerability cases (software malfunctions)
 - Bots / ‘Robot’ software
 - Collusion / Chip dumping or other poker-related violations
 - False claims
 - Circumvention of wagering limitations

Benefits for operators:

- Enhanced player trust
- Satisfies license conditions under new Curacao compliance regulations

LOK Requirements:

There are rules and processes set with specified time frames set in the new Gaming law in how to handle player’s complaints and these should be always available to players by the operators.

3. Self-Exclusion Services

Self-exclusion is a responsible gambling measure that allows players to voluntarily ban themselves from accessing online gambling services for a specific period—or permanently. During this time, the operator is obligated to block access to the account and prevent any marketing communication with the excluded individual.

Why is Self-Exclusion Needed?

- 1. Protects Vulnerable Players:** Gambling can become addictive. Self-exclusion helps individuals who recognize they may have a gambling problem take control by removing access to gambling platforms.
- 2. Reduces Harmful Behavior:** It prevents impulsive gambling decisions, especially after losses (chasing losses), which often exacerbate addiction and financial harm.
- 3. Mental Health and Financial Safety:** People struggling with gambling addiction often face anxiety, depression, debt, or family breakdown. Self-exclusion helps minimize these risks.
- 4. Supports Responsible Gambling:** It shows that the gaming operator is committed to ethical practices, not just profit.
 - Centralized exclusion database across participating platforms
 - Real-time user status API to prevent access
 - Player-led exclusion portal
 - Operator dashboard for flagging problem behaviors

Compliance edge: Helps meet responsible gaming requirements and align with Curacao gaming law and international compliance frameworks.

LOK Requirement: All operators should have policies and processes in place to safeguard the responsible offering of games of chance, grant players the opportunity to self-exclude from playing games of chance according to specified times frames set in the LOK.

4. Digital Record-Keeping and Player Backup Services

Curaçao is home to the only Tier-IV certified data center in the Caribbean, operated by Blue NAP Americas. This facility, located in Willemstad, offers the highest level of reliability and redundancy for hosting critical infrastructure, making it an excellent choice for online

gaming operators seeking robust disaster recovery and compliance-ready hosting solutions.

A Tier-IV data center guarantees 99.995% uptime per year, meaning only about 26 minutes of downtime annually. It features:

- Dual independent power systems with 14-day fuel reserves.
- Fully redundant cooling systems with advanced leak detection.
- Hurricane-resistant infrastructure, designed to withstand Category 5 storms.
- Multiple fiber optic connections, including five international submarine cables.
- Advanced security measures, such as anti-climb walls and a concrete roof ballast system.

These features ensure continuous operations and data protection, which are critical for online gaming platforms that require high availability and compliance with regulatory standards.

- Encrypted digital vault for storing player activity logs
- Data redundancy and access logs
- Compliant with GDPR and Curaçao's evolving data retention standards
- Automated reporting engine for audits

LOK Requirement: Each operator must maintain an operations manual containing information about the manner and degree of compliance with the provisions laid down in LOK, which includes have player's data backed up at a Tier IV Data Center in Curacao.

Market Analysis

Industry Trends

- Increased regulatory scrutiny in iGaming
- Growing demand for transparent compliance mechanisms
- Rising player awareness of safety and fairness standards

Target Market

- iGaming operators licensed in Curaçao
- New market entrants seeking licensing support
- Platform providers and white-label services
- Existing operators needing ADR or data compliance upgrades

Competitive Edge

- First-mover advantage with real-time compliance seal (Live Heartbeat Seal)
 - Modular service packages (customizable per operator size)
 - Deep regulatory expertise specific to Curaçao
-

Revenue Model

1. **Subscription-based packages** for operators (monthly/annual)
 2. **Per-incident fees** for dispute resolution (outside subscription)
 3. **Licensing of Live Heartbeat Seal** as a standalone product
 4. **Custom consulting fees** for alias and structuring work
-

Marketing Strategy

- **B2B Partnerships** with Curacao license agents and law firms
 - **Content marketing:** Regulatory updates, whitepapers, webinars
 - **Presence at gaming expos** (e.g., iGB Live, ICE Barcelona, Sigma)
 - **Referral program** for agents and consultants
-

Technology Stack

- **Secure cloud infrastructure** (AWS/GCP) with data residency compliance
 - **Custom-built dashboard** for operators
 - **REST API access** for integration with operator platforms
 - **End-to-end encryption** on all data and communication
-

Operations Plan

Staffing:

- Legal & Compliance Team (2)
- Technical Developers (2)
- Support & Dispute Handlers (2)
- Sales/Client Managers (1)

Key Partners:

- Local law firms
 - Payment and hosting providers
 - Compliance software vendors
 - Corporate Service Providers/Managing Directors
-

Financial Projections (3 years)

	Year 1	Year 2	Year 3
Revenue	\$ 270,000.00	\$ 351,000.00	\$ 459,000.00
IT Expenses	\$ 102,000.00	\$ 108,000.00	\$ 120,000.00
Employees	\$ 102,000.00	\$ 132,000.00	\$ 162,000.00
Office	\$ 24,000.00	\$ 24,000.00	\$ 24,000.00
License	\$ 30,000.00	\$ 30,000.00	\$ 30,000.00
Net	\$ 12,000.00	\$ 57,000.00	\$ 123,000.00

Risk Assessment

Risk	Mitigation
Regulatory changes	Legal advisor onboard + agile services
Data breaches	Encrypted storage & regular audits
Market competition	Unique value with Live Seal + bundles
Client churn	Strong onboarding + performance metrics

Next Steps

1. Finalize service architecture and packages
 2. Launch website and client onboarding portal
 3. Begin pilot testing with early adopter clients
 4. Scale marketing and sales across key markets
-

1. Understanding License Compliance

License compliance generally involves ensuring that software is being used in accordance with the terms and conditions set out in licensing agreements. This can apply to both software products your company owns and any third-party software you use. The goal is to ensure that your organization doesn't face legal risks due to unlicensed software, incorrect usage, or violations of intellectual property laws.

Here's a breakdown of what this process typically involves:

- **Software Inventory Management:**
 - Maintain an accurate and up-to-date inventory of all software in use across the organization.
 - Document software purchases, subscriptions, and licenses, including the number of users, version information, and renewal dates.
 - Ensure software is only installed on authorized machines or devices.
- **Regular Audits and Reviews:**
 - Perform regular internal audits to review the software inventory.
 - Conduct periodic reviews of your organization's license usage to ensure that you aren't over-licensed or under-licensed.
 - Review license agreements and terms periodically for any changes or renewals that need to be addressed.
- **Vendor Communications:**
 - Keep in touch with software vendors to stay informed about any license updates, changes, or new agreements.
 - Ensure that you're aware of renewal dates and any potential license compliance checks from the vendor.
- **Software Usage Monitoring:**
 - Use tools or software management platforms to track actual usage versus purchased licenses.
 - Identify and eliminate any unauthorized installations or excess installations.

2. Corporate Compliance Reviews

Corporate compliance, on the other hand, covers the broader scope of ensuring that your business is following all applicable laws, industry standards, and internal policies. This includes data privacy laws, financial reporting, health and safety regulations, and so on.

The ongoing corporate compliance review process usually includes:

- **Regulatory Compliance:**

- Ensure the company is in compliance with all relevant local, regional, and international laws (LOK, GDPR etc.).
- Identify industry-specific regulations that need to be adhered to.
- Track any changes in regulations that could impact your organization.

- **Internal Audits:**

- Conduct regular internal audits across different departments (finance, IT, HR, legal, etc.).
- Ensure that internal policies are being followed (e.g., codes of conduct, anti-bribery policies, conflict of interest rules).
- Ensure that financial reporting is accurate and follows accounting standards.

- **Risk Management:**

- Review risk management frameworks and processes to ensure that potential risks are being identified and mitigated.
- Assess whether your compliance controls are effective at reducing risks, especially around data security and privacy.

- **Employee Training and Awareness:**

- Ensure that employees are properly trained on compliance-related matters (e.g., data privacy, ethics, legal obligations).
- Reinforce the importance of compliance through periodic training sessions or awareness campaigns.

- **Reporting & Documentation:**

- Maintain a clear record of compliance efforts, audits, and any corrective actions taken.
- Create reports for senior management and any external stakeholders (investors, regulators, etc.).

3. Best Practices for Ongoing Compliance Reviews

- **Centralize Compliance Management:** Consider using a compliance management platform to centralize your records for both licenses and broader corporate compliance. This will help automate reminders for renewals, audits, and tracking compliance activities.
- **Implement Continuous Monitoring:** Instead of relying only on periodic reviews, use automated tools for continuous monitoring of software and corporate compliance. This will help identify issues in real-time and prevent violations before they occur.
- **Regular Updates:** Keep all documentation and licenses up-to-date, especially when there are changes in regulations or when new software is acquired.
- **Cross-department Collaboration:** License compliance often involves IT teams, procurement, legal, and finance departments. Corporate compliance reviews will typically involve various departments as well (e.g., legal, HR, IT). Foster collaboration across these teams to ensure a comprehensive review process.
- **Documentation and Corrective Action:** Ensure that any findings from compliance reviews are documented, and that corrective actions are taken quickly. This may include updating processes, renewing licenses, or conducting employee training.

4. Tools and Resources for Compliance

- **Software Asset Management (SAM) Tools:** These tools help track software licenses and ensure compliance, including tracking usage, ensuring you don't over-deploy, and managing renewals.
- **GRC (Governance, Risk, and Compliance) Tools:** GRC platforms provide a centralized approach to managing compliance across various regulatory frameworks. They can automate risk assessments, audits, and reporting.
- **Contract Management Software:** Helps keep track of software agreements, renewals, and compliance with licensing terms.
 - Examples: Icertis, Agiloft, ContractWorks.
- **Compliance Frameworks:** Depending on your industry, you might need to follow specific frameworks such as ISO 27001, SOC 2, or PCI-DSS for data security, which may influence your compliance reviews.

Benefits

Trust & Transparency: Neutral handling builds player confidence

Compliance : Aligns with regulatory reforms and expectations

Risk Reduction: Avoid mishandling that could trigger legal or license issues

Efficiency: Saves internal resources and improves processing speed

Better Tools: Professional third parties offer more advanced handling systems