

The iGaming and Gambling Compliance Guide.

Nine jurisdictions. **One standard of compliance.**

The financial crime risks specific to online gambling, the AML obligations that apply everywhere, and the jurisdiction-specific requirements across the world's most important licensing hubs.

CONTENTS

Seventeen Chapters, Nine Jurisdictions, One Compliance Program

PART 1 · THE IGAMING FINANCIAL CRIME LANDSCAPE

1	Introduction: Compliance at the Center of iGaming	3
2	The iGaming Financial Crime Risk Profile	4

PART 2 · CORE COMPLIANCE OBLIGATIONS

3	Core Pillars of iGaming AML Compliance	5
----------	--	---

PART 3 · JURISDICTION-SPECIFIC REGULATIONS

4	United Kingdom (UKGC)	8
5	Malta (MGA)	10
6	Curaçao (CGA)	11
7	Sweden (Spelinspektionen)	12
8	Denmark (Spillemyndigheden)	13
9	Estonia	14
10	Gibraltar	15
11	Isle of Man (GSC)	16
12	Cyprus (NBA)	17

PART 4 · OPERATIONAL EXCELLENCE

13	The White-Label and B2B Compliance Challenge	18
14	Case Study: Together Gaming	19
15	Building a Future-Ready Compliance Program	20

CONCLUSION

16	Why sanctions.io Is Your Ideal Screening Partner	22
17	Your Next Steps	24
	Sources	25

— PART 1 · THE iGAMING FINANCIAL CRIME LANDSCAPE · CHAPTER 1

Introduction: Compliance at the Center of iGaming

The iGaming industry has undergone a remarkable transformation over the past decade. What began as a niche corner of the entertainment sector has evolved into a global, multi-billion-dollar industry spanning online casinos, sports betting, poker platforms, digital lotteries, and live dealer games. **With this growth has come an equally significant expansion in regulatory expectations.**

Today, compliance is not a peripheral administrative function for iGaming operators. It is a core operational requirement that determines whether a business can access and retain its licenses, maintain banking relationships, and build lasting trust with players and partners. Regulators across every major licensing jurisdiction are intensifying their scrutiny of Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) controls, and the consequences of failure are severe.

Between 2024 and 2025, European regulators issued tens of millions of euros in AML-related fines targeting gambling firms.¹ In the UK alone, the Gambling Commission issued multimillion-pound penalties to operators for significant gaps in AML controls.² These are not isolated incidents. They reflect a global regulatory direction that is firmly set toward higher standards, greater accountability, and more active enforcement.

This guide is designed for compliance professionals, legal teams, and senior executives working in or with the iGaming sector. It provides a comprehensive overview of the financial crime risks specific to online gambling, the core compliance obligations that apply universally, and the jurisdiction-specific requirements that operators must understand across nine of the most important licensing and market-access jurisdictions in the world.

PART 1 · THE iGAMING FINANCIAL CRIME LANDSCAPE · CHAPTER 2

The iGaming Financial Crime Risk Profile

Understanding why the iGaming sector attracts such intense regulatory attention requires a clear-eyed assessment of the financial crime risks that are inherent to the industry.

The Financial Action Task Force (FATF) classifies casinos and internet-based (online) casinos as Designated Non-Financial Businesses and Professions (DNFBPs), placing them alongside accountants, lawyers, and real estate agents as sectors with elevated vulnerability to money laundering.³ The nature of online gambling, characterized by high transaction volumes, cross-border financial flows, non-face-to-face customer relationships, and the rapid movement of funds, creates a highly attractive environment for illicit actors seeking to integrate criminal proceeds into the legitimate financial system.

The three stages, applied to iGaming

1 Placement Illicit funds are introduced into the gambling ecosystem, often via prepaid cards, compromised bank accounts, or virtual currencies that obscure the source of wealth.	2 Layering Funds are wagered in a manner designed to obscure their origin: chip dumping in peer-to-peer games, minimal bets on low-risk outcomes, or rapid transfers between operator accounts.	3 Integration Funds are withdrawn from the platform and, because the withdrawal appears as a legitimate payout from a licensed operator, are successfully reintroduced into the legitimate economy.
--	---	---

Beyond traditional money laundering, iGaming operators face distinct typologies of financial crime. Other types of financial exploitation involve the creation of synthetic identities or the use of stolen credentials to exploit promotional offers.⁴ The exploitation of VIP programs remains a persistent risk, as operators may be incentivized to lower compliance friction for high-value players. Furthermore, the increasing adoption of cryptocurrencies as a funding method introduces additional complexity, requiring specialized blockchain analytics to trace the source of funds.

PART 2 · CORE COMPLIANCE OBLIGATIONS · CHAPTER 3

Core Pillars of iGaming AML Compliance

Business risk assessment

The foundation of any AML program is a documented Business Risk Assessment. This is not a one-time exercise. It must be reviewed and updated regularly to reflect changes in the business model, customer demographics, product offerings, payment methods, and the broader regulatory environment. The risk assessment should identify the specific money laundering and terrorist financing risks the operator faces and inform the design of all downstream controls.

To get started with assessing business risk, you can use our free, 3-minute **Global Risk Exposure Calculator** to discover your screening risks and requirements.

Customer Due Diligence (CDD)

Customer Due Diligence is the process by which operators verify the identity of their players and assess the risk they present. At a minimum, this involves collecting and validating personal information, confirming the customer's identity against reliable and independent sources, and assessing their risk profile based on factors such as their country of residence, payment methods, and transaction patterns. CDD must be completed before a customer is permitted to engage in significant transactions, and it must be refreshed throughout the relationship as circumstances change.

Enhanced Due Diligence (EDD)

Enhanced Due Diligence applies to customers who present a higher risk of money laundering or terrorist financing. This includes Politically Exposed Persons (PEPs), customers from high-risk jurisdictions, those with complex ownership structures, and individuals who have triggered suspicious activity alerts. EDD typically involves obtaining additional documentation, verifying the source of funds and source of wealth, conducting PEP checks, and applying more frequent and intensive ongoing monitoring.⁵

Sanctions and PEP screening

Every customer must be screened against applicable sanctions lists and PEP databases at onboarding and on a continuous basis thereafter. This is a non-negotiable requirement across all jurisdictions, particularly where US, UK, or EU jurisdictions are involved.⁵ PEP screening is equally important, as politically exposed individuals present elevated risks of bribery and corruption even when they are not formally sanctioned; it is typically risk-based and most commonly applied as part of Enhanced Due Diligence for higher-risk customers.

Critically, initial screening at onboarding is only the starting point. Operators must also maintain continuous monitoring: automatically and repeatedly checking customers against sanctions lists and watchlists, for example every 60 minutes, with re-screening triggered whenever a customer's status changes or new sanctions designations are issued.

Transaction monitoring

Ongoing transaction monitoring is essential for detecting unusual player behavior that may indicate money laundering or other financial crime. Operators must track patterns such as large deposits followed by immediate withdrawals with minimal gameplay, structured deposits designed to stay below reporting thresholds, rapid transfers between accounts, and unusual betting patterns inconsistent with a player's declared income or gambling history.

Suspicious Activity Reporting (SAR)

When suspicious activity is identified, operators are legally obligated to file Suspicious Activity Reports with the relevant Financial Intelligence Unit. These reports must be detailed, timely, and based on a genuine assessment of the facts rather than a formulaic response to a system alert. Failure to report suspicious activity can result in serious regulatory and criminal consequences.

Record keeping and governance

Operators must maintain comprehensive records of customer identification, transaction histories, due diligence documentation, and SAR filings for a minimum of five years in most jurisdictions.²⁵ Governance arrangements typically include a designated Money Laundering Reporting Officer (MLRO), clear escalation procedures, regular AML training for all relevant staff, and independent oversight of the compliance function.

The seven pillars

1 Business risk assessment	2 Customer Due Diligence
3 Enhanced Due Diligence	4 Sanctions and PEP screening
5 Transaction monitoring	6 Suspicious Activity Reporting
7 Record keeping and governance	

UNIVERSAL

These pillars apply in every jurisdiction covered in Part 3. The differences lie in thresholds, regulators and enforcement style, not in the fundamentals.

PART 3 · JURISDICTION-SPECIFIC REGULATIONS

Nine Jurisdictions, Nine Regimes

While the core compliance pillars apply universally, iGaming operators must navigate the specific legal and regulatory requirements of each jurisdiction where they hold a license or accept players. The nine jurisdictions covered in this section represent some of the most important licensing hubs and regulated markets in the global iGaming industry.

PART 3 · JURISDICTION-SPECIFIC REGULATIONS · CHAPTER 4

United Kingdom (UKGC)

The UK Gambling Commission (UKGC) maintains one of the most prescriptive and actively enforced regulatory regimes in the world. Under the Money Laundering Regulations 2017, remote and non-remote casinos are explicitly classified as part of the regulated sector for AML purposes.⁶ Other gambling operators, while not subject to the full MLR regime, still carry significant obligations under the Proceeds of Crime Act 2002, the Terrorism Act 2000, and the UKGC's Licence Conditions and Codes of Practice.

The UKGC framework is notable for how operational and dynamic it has become. The Commission publishes a dedicated AML hub, sector risk assessments, emerging risk bulletins, and regular guidance updates. Operators are expected not only to have a policy in place but to keep it current in light of supervisory publications.

The Commission’s November 2025 casino guidance update introduced several significant changes, including updated PEP guidance, revised high-risk third country lists, an increase in the DAML threshold to £3,000, and explicit expectations that operators must assess the AML risks posed by B2B relationships, white-label partners, and third-party providers.⁷ The Commission’s April 2025 emerging risk bulletin further highlighted risks including payments from PEPs or sanctioned persons, customers using multiple payment methods, reliance on third-party due diligence, and the use of AI-generated deepfakes and face swaps to bypass identity verification.⁸

The UKGC has demonstrated a clear willingness to enforce these standards. In 2025 alone, ProgressPlay Limited received a £1 million fine for failing to properly verify player funds, and Platinum Gaming Limited received a £10 million penalty for significant gaps in AML and safer gambling controls.²

KEY REQUIREMENTS AT A GLANCE

Regulator	UK Gambling Commission (UKGC)
Legal basis	Money Laundering Regulations 2017; POCA 2002; Terrorism Act 2000
Scope	Remote and non-remote casinos (regulated sector); all other operators (broader obligations)
Key obligations	Business risk assessment, CDD, EDD for PEPs, sanctions screening, SAR filing, MLRO
Recent developments	November 2025 casino guidance update; April 2025 emerging risk bulletin

PART 3 · JURISDICTION-SPECIFIC REGULATIONS · CHAPTER 5

Malta (MGA)

Malta is one of the most established licensing hubs for remote gaming globally, and its AML regime reflects that maturity. The Malta Gaming Authority (MGA) acts as the supervisory authority for AML compliance in conjunction with the Financial Intelligence Analysis Unit (FIAU). AML and CFT obligations apply specifically to B2C licensees offering Type 1, 2, and 3 gaming services, encompassing casinos, sports betting, and peer-to-peer gaming.⁹

The Maltese framework is grounded in the Prevention of Money Laundering Act and the Prevention of Money Laundering and Funding of Terrorism Regulations (PMLFTR). The FIAU’s Implementing Procedures Part II for the Remote Gaming Sector provides detailed, sector-specific guidance on how operators must fulfill these obligations.¹⁰

Key requirements include the appointment of a dedicated MLRO based in Malta, the implementation of a comprehensive Customer Risk Assessment methodology, and strict adherence to CDD requirements when player deposits reach €2,000 in a rolling 180-day period. The FIAU is an active enforcer, frequently issuing administrative penalties for failures related to inadequate risk assessments, insufficient source of wealth checks, and delayed SAR reporting.¹¹

KEY REQUIREMENTS AT A GLANCE

Regulator	Malta Gaming Authority (MGA) and FIAU
Legal basis	Prevention of Money Laundering Act; PMLFTR; FIAU Implementing Procedures Part II
Scope	B2C licensees (Type 1, 2, 3 gaming services)
Key obligations	MLRO appointment, Customer Risk Assessment, CDD at €2,000 threshold, EDD, SAR reporting
Recent developments	Active FIAU enforcement; ongoing alignment with EU 6AMLD

PART 3 · JURISDICTION-SPECIFIC REGULATIONS · CHAPTER 6

Curaçao (CGA)

Curaçao is currently undergoing a fundamental transformation of its gambling regulatory framework. Historically operating under a master license and sub-license model that faced international criticism for perceived laxity, the jurisdiction introduced the National Ordinance for Games of Chance (LOK) in December 2024 to establish a direct licensing system under a new regulator, the Curaçao Gaming Authority (CGA).¹²

This transition represents a significant tightening of AML and CFT standards. Under the LOK framework, all operators must apply directly to the CGA for a license and demonstrate robust compliance infrastructure. The new regime mandates stringent CDD and EDD procedures, mandatory sanctions and PEP screening, and the implementation of automated transaction monitoring systems.¹³

Operators previously operating under sub-licenses must adapt rapidly to these elevated expectations. The CGA has made it clear that basic, manual compliance checks will no longer suffice, particularly given the jurisdiction’s historical association with high-risk payment methods and cryptocurrency operators.

KEY REQUIREMENTS AT A GLANCE

Regulator	Curaçao Gaming Authority (CGA)
Legal basis	National Ordinance for Games of Chance (LOK)
Scope	All licensed online gambling operators
Key obligations	CDD, EDD, sanctions and PEP screening, automated transaction monitoring
Recent developments	Full transition from master/sub-license model; elevated AML standards under LOK

PART 3 · JURISDICTION-SPECIFIC REGULATIONS · CHAPTER 7

Sweden (Spelinspektionen)

The Swedish Gambling Authority (Spelinspektionen) regulates the commercial online gambling and betting market under the Gambling Act (2018:1138). Swedish licensees are fully subject to the national Anti-Money Laundering Act (2017:630), which implements the EU AML Directives.¹⁴

Sweden’s regulatory approach is characterized by strict consumer protection and rigorous enforcement of AML obligations. Operators must conduct comprehensive risk assessments, implement robust CDD procedures, and utilize the Swedish BankID system for secure player authentication where applicable.

Spelinspektionen takes a zero-tolerance approach to compliance failures. The authority regularly issues substantial fines and warnings to operators for deficiencies in their AML frameworks, particularly regarding inadequate risk assessments, failure to conduct sufficient source of funds checks on high-spending players, and delays in reporting suspicious transactions to the Swedish Financial Intelligence Unit.¹⁵

KEY REQUIREMENTS AT A GLANCE

Regulator	Spelinspektionen
Legal basis	Gambling Act (2018:1138); Anti-Money Laundering Act (2017:630)
Scope	All licensed commercial online gambling and betting operators
Key obligations	Risk assessments, CDD, BankID authentication, source of funds checks, SAR reporting
Recent developments	Active enforcement; zero-tolerance approach to AML deficiencies

PART 3 · JURISDICTION-SPECIFIC REGULATIONS · CHAPTER 8

Denmark (Spillemyndigheden)

The Danish Gambling Authority (Spillemyndigheden) oversees a well-regulated market where operators must comply with the Danish Anti-Money Laundering Act. The Danish regime places a strong emphasis on detailed risk assessments, robust CDD, and proactive suspicious activity reporting to the Money Laundering Secretariat.¹⁶

A defining feature of the Danish framework is the requirement for operators to implement stringent player verification procedures, often leveraging the national MitID digital identity system. Operators are also expected to maintain a highly detailed understanding of player behavior and to intervene swiftly when unusual patterns emerge.

Spillemyndigheden is known for its rigorous supervisory approach, frequently conducting thematic reviews and on-site inspections. The authority has issued numerous reprimands and orders to operators for failing to adequately document their risk assessment methodologies or for maintaining insufficient transaction monitoring capabilities.

KEY REQUIREMENTS AT A GLANCE

Regulator	Spillemyndigheden
Legal basis	Danish Anti-Money Laundering Act
Scope	All licensed gambling operators in Denmark
Key obligations	Risk assessments, CDD, MitID verification, transaction monitoring, SAR reporting
Recent developments	Thematic reviews and on-site inspections; active enforcement

PART 3 · JURISDICTION-SPECIFIC REGULATIONS · CHAPTER 9

Estonia

Estonia has emerged as a forward-looking jurisdiction that actively accommodates technological innovation, including the use of cryptocurrencies, while maintaining strict regulatory standards. The Estonian Tax and Customs Board is responsible for issuing gambling licenses, while the Financial Intelligence Unit (FIU) oversees AML compliance.

Licensed operators are subject to the Money Laundering and Terrorist Financing Prevention Act, which mandates comprehensive risk assessments, CDD, EDD, and SAR reporting. The Estonian FIU is particularly focused on the risks associated with virtual assets and cross-border transactions.

Recent developments indicate a tightening of the regulatory environment. The FIU has increasingly focused on the gambling sector's exposure to international sanctions evasion, including risks associated with Russia, Belarus, Georgia, and Uzbekistan, and the growing acceptance of cryptocurrency deposits and withdrawals.¹⁷

KEY REQUIREMENTS AT A GLANCE

Regulator	Estonian Tax and Customs Board (licensing); Financial Intelligence Unit (AML)
Legal basis	Money Laundering and Terrorist Financing Prevention Act
Scope	All licensed gambling operators in Estonia
Key obligations	Risk assessments, CDD, EDD, virtual asset monitoring, SAR reporting
Recent developments	Increased FIU focus on sanctions evasion and cryptocurrency risks

PART 3 · JURISDICTION-SPECIFIC REGULATIONS · CHAPTER 10

Gibraltar

Gibraltar has long been a respected jurisdiction for remote gambling, known for its rigorous regulatory standards and its status as a British Overseas Territory. The Gibraltar Gambling Commissioner oversees the sector under the Gambling Act 2005, with a new Gambling Act enacted in 2026 to modernize the framework.¹⁸

Gibraltar’s removal from the FATF grey list in February 2024 was a significant milestone that reinforced the jurisdiction’s credibility as a well-regulated hub. Operators are required to comply with Gibraltar’s AML Code, which mandates comprehensive CDD, EDD, PEP screening, and SAR reporting obligations. The Remote Technical Operating Standard sets additional requirements for the technical infrastructure of online gambling operations.¹⁹

Gibraltar’s regulatory environment is particularly attractive to premium operators seeking a credible, English-law jurisdiction with strong international recognition. The jurisdiction’s small size enables close regulatory relationships and a pragmatic, risk-based supervisory approach.

KEY REQUIREMENTS AT A GLANCE

Regulator	Gibraltar Gambling Commissioner (Gambling Division)
Legal basis	Gambling Act 2005 (new Act effective 2026)
Scope	All remote and land-based gambling operators in Gibraltar
Key obligations	AML Code compliance, Remote Technical Operating Standard, CDD, PEP screening
Recent developments	Removed from FATF grey list February 2024; new Gambling Act enacted 2026

PART 3 · JURISDICTION-SPECIFIC REGULATIONS · CHAPTER 11

Isle of Man (GSC)

The Isle of Man Gambling Supervision Commission (GSC) provides rigorous oversight of the online gambling sector under the Online Gambling Regulation Act. The jurisdiction’s AML framework is governed by the Gambling (Anti-Money Laundering and Countering the Financing of Terrorism) Code 2019, which requires all operators to conduct comprehensive business risk assessments and implement controls commensurate with the risks identified.²⁰

The GSC is an active regulator that regularly updates its guidance to reflect emerging risks and international best practices. In October 2025, the Commission released updated AML guidance specifically for online gambling licence holders with network services, addressing the compliance responsibilities that arise from complex multi-operator arrangements.²¹

KEY REQUIREMENTS AT A GLANCE

Regulator	Gambling Supervision Commission (GSC)
Legal basis	Online Gambling Regulation Act; Gambling (AML and CFT) Code 2019
Scope	All online gambling licence holders
Key obligations	Business risk assessment, CDD, EDD, SAR reporting, MLRO appointment
Recent developments	Updated AML guidance for network service operators (October 2025)

PART 3 · JURISDICTION-SPECIFIC REGULATIONS · CHAPTER 12

Cyprus (NBA)

In Cyprus, the National Betting Authority (NBA) regulates the betting sector under the Betting Law 37(I)/2019 and serves as the supervisory authority for AML compliance in the industry.²² The NBA works alongside MOKAS, the Unit for Combating Money Laundering, which is Cyprus's national FIU.

Operators licensed in Cyprus face strict obligations to appoint a dedicated compliance officer, implement CDD and EDD procedures, monitor transactions for suspicious activity, and file SARs with MOKAS. The NBA has been increasingly active in issuing directives that clarify and strengthen AML expectations for licensees, reflecting the broader EU trend toward more demanding compliance standards.

KEY REQUIREMENTS AT A GLANCE

Regulator	National Betting Authority (NBA)
Legal basis	Betting Law 37(I)/2019
Scope	All licensed betting operators in Cyprus
Key obligations	Compliance officer appointment, CDD, EDD, transaction monitoring, SAR filing with MOKAS
Recent developments	Increased NBA directives strengthening AML expectations

PART 4 · OPERATIONAL EXCELLENCE · CHAPTER 13

The White-Label and B2B Compliance Challenge

A critical area of regulatory focus across multiple jurisdictions is the compliance responsibility inherent in white-label and B2B arrangements. In a white-label structure, a licensed operator provides the platform, gaming content, and regulatory umbrella, while a third-party brand partner handles marketing and customer acquisition.

Regulators, notably the UKGC and the MGA, have made it unequivocally clear that the licensed operator retains ultimate responsibility for AML compliance, regardless of how operational tasks are delegated.²³ The licensee must ensure that all CDD, EDD, and screening procedures meet regulatory standards, even if the brand partner is the primary point of contact with the customer.

This creates significant operational challenges. Licensees must implement robust oversight mechanisms to monitor the compliance performance of their brand partners. They must ensure that data flows seamlessly between the brand interface and the core compliance systems, enabling real-time screening and transaction monitoring. Failures in these B2B arrangements have been a primary driver of recent regulatory enforcement actions, highlighting the need for fully integrated, API-driven compliance infrastructure that spans the entire operator ecosystem.

AT THE INTERSECTION OF GAMING AND PAYMENTS?

Download The FinTech Compliance Playbook for actionable steps, best practices, and real cases of sanctions compliance.

PART 4 · OPERATIONAL EXCELLENCE · CHAPTER 14

Case Study: Together Gaming and the Path to Scalable Compliance

The practical challenges of iGaming compliance are best illustrated through real-world experience. Together Gaming, a large white-label iGaming developer, encountered a set of compliance challenges that are common across the industry as businesses scale.²⁴

The company's existing compliance infrastructure relied on inflexible, subcontracted legacy solutions that created significant operational friction. Pricing structures for ongoing monitoring were prohibitive at scale, and the lack of real-time feedback made it difficult for AML teams to respond promptly to emerging risks. As Together Gaming's customer base grew, these limitations became increasingly untenable.

By transitioning to a fully integrated, API-based screening solution with sanctions.io, Together Gaming achieved a 5x reduction in false positives at scale. The new infrastructure delivered operational efficiency and peace of mind for AML teams, and critically, it provided a compliance capability that could scale alongside the business's aggressive growth trajectory.²⁴

5x
FEWER FALSE
POSITIVES

"The integration was flawless. The response times from the team were impressive every time. Using you guys put that puzzle out of our head, we don't need to think much about this particular side of the business."

Vilius Balciunas, COO, Together Gaming

The Together Gaming case study illustrates a broader truth about iGaming compliance: the technology underpinning a compliance program matters as much as the policies and procedures. Operators that invest in modern, API-driven screening infrastructure are better positioned to meet regulatory expectations, respond to emerging risks, and grow their businesses without compliance becoming a bottleneck. **Read the full Together Gaming case study.**

PART 4 · OPERATIONAL EXCELLENCE · CHAPTER 15

Building a Future-Ready Compliance Program

As regulatory demands increase and transaction volumes grow, the iGaming operators best positioned for long-term success will be those that **treat compliance as a strategic investment rather than a cost center.**

Technology integration

Manual compliance processes are no longer viable at scale. Modern iGaming compliance requires scalable, smart screening infrastructure that integrates directly with player management systems, payment processors, and back-office platforms through API-driven screening or native, low-code integrations. Real-time screening, automated alert generation, and seamless data flows between systems are the baseline expectation of regulators and the operational reality of high-volume operators. Evaluating new compliance technology? Download our **Vendor Selection Guide** to learn the top features to look for in a sanctions screening solution.

Continuous monitoring

Compliance should not be limited to a point-in-time activity. Sanctions lists are updated daily, PEP databases change constantly, and customer risk profiles evolve over time. Operators must implement continuous monitoring capabilities that automatically re-screen customers whenever relevant data changes, rather than relying on periodic batch reviews that may miss critical updates.

Data quality and coverage

The effectiveness of any screening program is only as good as the data it uses. Operators must ensure that their screening solutions draw on comprehensive, regularly updated sanctions lists, PEP databases, and adverse media sources. Coverage gaps, outdated data, or poor name-matching algorithms can result in missed hits, creating both regulatory and reputational risk.

Governance and culture

Technology alone is not sufficient. A future-ready compliance program requires a culture of compliance that permeates the entire organization, from the board level to front-line customer service staff. This means regular training, clear accountability structures, robust escalation procedures, and a genuine commitment from senior leadership to prioritize compliance as a strategic function.

CONCLUSION · CHAPTER 16

Why sanctions.io Is Your Ideal Screening Partner

Building a strong iGaming compliance program requires more than basic screening. It requires a platform that can help your team identify sanctions exposure, assess reputational risk, reduce false positives, and operationalize screening across player onboarding, ongoing monitoring, and B2B partner workflows.

Comprehensive risk coverage

sanctions.io helps iGaming operators screen players and partners against global sanctions lists, PEP data, criminal watchlists, and adverse media sources drawn from 100+ data sources, giving compliance teams a broader and more actionable view of financial crime risk.

Built for operational workflows

Whether you are screening players during onboarding, reviewing VIP accounts, assessing white-label partners, or monitoring counterparties in real time, sanctions.io can be embedded directly into the systems your teams already use, including Microsoft Dynamics 365, HubSpot, Salesforce, BigID, SAP, and via API.

**Smarter matching,
fewer bottlenecks**

Effective iGaming compliance depends on accuracy as much as coverage. sanctions.io uses ML and AI-powered matching to handle name variation, transliteration issues, and common false-positive scenarios, delivering a significant reduction in false positives so your compliance team can focus on the alerts that matter most.

**Monitoring that keeps
pace with risk**

Player and partner risk does not stop at onboarding. With sanctions lists and data updated every 60 minutes, continuous monitoring and real-time alerts, sanctions.io helps operators stay informed when a customer's or partner's risk profile changes after the relationship has already begun.

Scalable for growth

From lean compliance teams to large multi-brand operations, sanctions.io helps iGaming businesses build screening processes that are proportionate, auditable, and ready to scale as player volumes and partner ecosystems grow. With a 99.995% SLA uptime guarantee and transparent pricing, you can explore costs upfront using the **sanctions.io pricing calculator**.

With sanctions.io, iGaming compliance screening becomes a practical control that supports both regulatory confidence and commercial growth.

— CONCLUSION · CHAPTER 17

Your Next Steps

With sanctions.io, you can build an iGaming compliance program that is faster, more consistent, and better aligned to today's sanctions and financial crime risk environment.

-
- 1** Assess your current state. Review how your organization currently screens players, VIP accounts, white-label partners, and payment providers. Identify where you rely on one-time checks, where monitoring gaps exist, and where false positives are slowing down your compliance team.
 - 2** Understand your risk exposure. Not sure where to start? Use the free **Global Risk Screening Calculator** to get a clear picture of your screening risks and requirements in under 3 minutes.
 - 3** Prioritize your highest-risk relationships. Start by reviewing the players and partners that create the greatest exposure, such as high-value VIP accounts, cross-border payment providers, and white-label operators in higher-risk jurisdictions. Apply stronger screening, clearer escalation rules, and ongoing monitoring where the risk is most material. For a structured approach to managing these relationships, download the **Third-Party Risk Screening Guide**, a practical resource for identifying, prioritizing, and managing high-risk third-party exposure.
 - 4** Book a call. If you are ready to strengthen your iGaming compliance program, **schedule a call** with the sanctions.io team to discuss your workflow, risk exposure, and implementation priorities.
-

Book a call

Prefer to talk it through? See how your compliance process can go from inefficient to simple, scalable and unified.

REFERENCES

Sources

- 1 **AML Watcher, Biggest AML Fines of 2025 (2025)**
amlwatcher.com
- 2 **UK Gambling Commission, Regulatory Action (2025)**
gamblingcommission.gov.uk/public-register/regulatory-action
- 3 **Financial Action Task Force (FATF), Vulnerabilities of Casinos and Gaming Sector**
fatf-gafi.org/en/publications/Methodsandtrends/Vulnerabilitiesofcasinosandgamingsector.html
- 4 **sanctions.io, Casino AML Compliance Guide (2025)**
sanctions.io/blog
- 5 **sanctions.io, Sanctions Compliance in the Gaming Industry (2024)**
sanctions.io/blog
- 6 **UK Government, The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017**
legislation.gov.uk/uksi/2017/692/contents
- 7 **UK Gambling Commission, AML Guidance for Casinos (2025)**
gamblingcommission.gov.uk/licensees-and-businesses/guide/anti-money-laundering
- 8 **UK Gambling Commission, Emerging Money Laundering and Terrorist Financing Risks Bulletin (2025)**
gamblingcommission.gov.uk/licensees-and-businesses/guide/anti-money-laundering
- 9 **Malta Gaming Authority, AML/CFT Information (2025)**
mga.org.mt/aml-cft
- 10 **Financial Intelligence Analysis Unit (FIAU), Implementing Procedures Part II, Remote Gaming Sector (2025)**
fiaumalta.org/publications/implementing-procedures
- 11 **sanctions.io, AML Screening and Regulations for iGaming: MGA, UKGC, and Curaçao (2024)**
sanctions.io/blog
- 12 **Curaçao Gaming Authority, National Ordinance for Games of Chance (LOK) (2025)**
gamingauthority.cw
- 13 **iGaming Business, Curaçao's New Gambling Law Explained (2024)**
igamingbusiness.com

-
- 14** **Spelinspektionen, Anti-Money Laundering (2025)**
spelinspektionen.se
-
- 15** **Spelinspektionen, Decisions and Sanctions (2025)**
spelinspektionen.se
-
- 16** **Spillemyndigheden, Anti-Money Laundering (2025)**
spillemyndigheden.dk
-
- 17** **Chambers and Partners, Gaming Law 2025: Estonia Trends and Developments (2025)**
practiceguides.chambers.com
-
- 18** **Gibraltar Gambling Commissioner, The Gambling Act 2026 (2026)**
gibraltar.gov.gi/finance-gaming-and-regulations/gambling
-
- 19** **Advennt, Online Gaming: Gibraltar Risk Assessment (2025)**
advennt.com
-
- 20** **Isle of Man Gambling Supervision Commission, Anti-Money Laundering (2025)**
gov.im/gsc
-
- 21** **Isle of Man Gambling Supervision Commission, Updated AML Guidance for Network Services (2025)**
gov.im/gsc
-
- 22** **National Betting Authority Cyprus, AML/CFT Framework (2025)**
nba.gov.cy
-
- 23** **UK Gambling Commission, White-label operations (2024)**
gamblingcommission.gov.uk
-
- 24** **sanctions.io, Case Study: Together Gaming's Journey to a Modern Screening Solution**
sanctions.io/resources/together-gaming-case-study
-
- 25** **UK Money Laundering Regulations 2017, Regulation 40; EU Fourth Anti-Money Laundering Directive (2015/849), Article 40**
legislation.gov.uk/uksi/2017/692/regulation/40
-