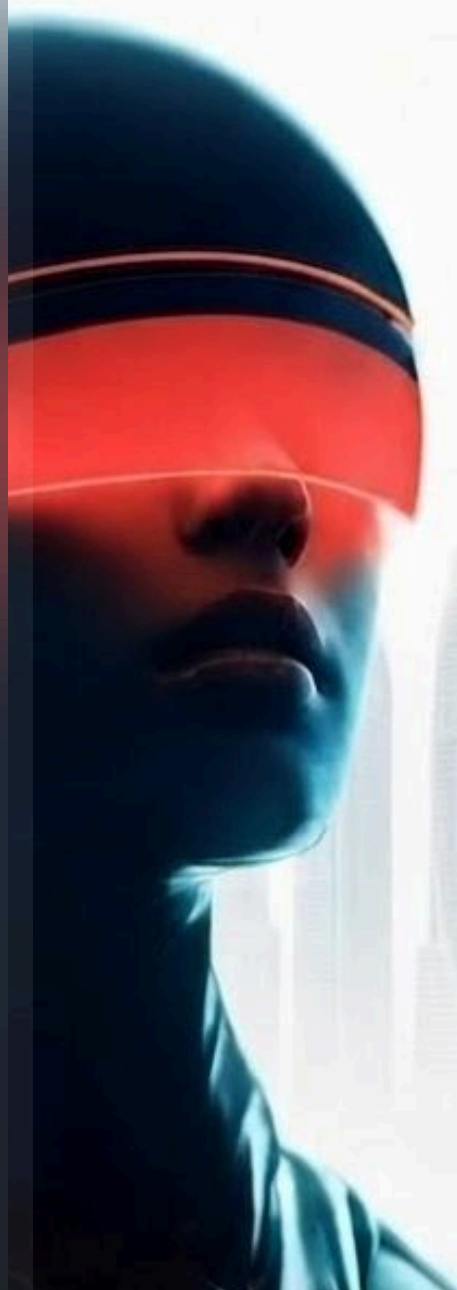


UAE Commercial Gaming Compliance Requirements

A Player Due Diligence and financial crime prevention
guide for iGaming operators

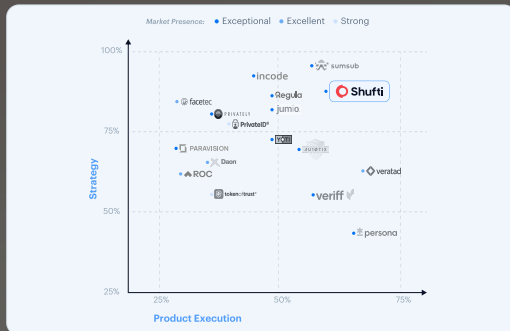


Industry Recognition 2025–2026

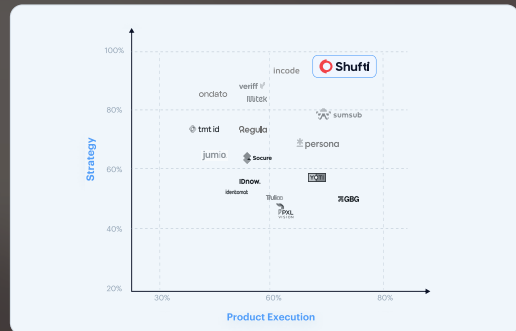
Recognised by leading analyst firms, government bodies and independent research organisations



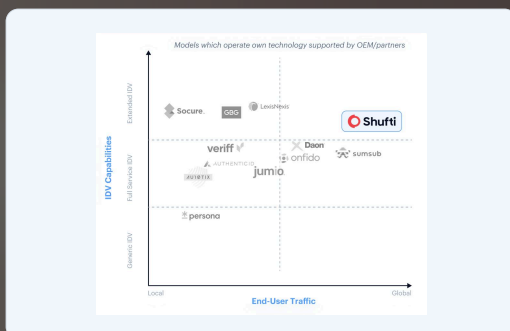
Ranked Exceptional in Liminal's 2026 Age Estimation Index



Ranked Exceptional in Liminal's 2026 Age Verification Index



Broadest global reach in the 2025 KuppingerCole Extended IDV report



Recognised as a Leader across four G2 Summer 2026 reports



Differentiated by Gartner on document diversity and country coverage



240+ Countries & Territories

10k+ Document Types

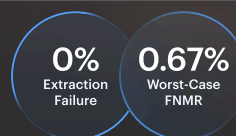


First EU company to achieve iBeta Level 3 Conformance to ISO/IEC 30107-3, with 0% APCER

iBeta Level 3 Conformance
0% APCER



Ranked Top 5 in the DHS RIVR 2025 for identity validation



KJM AGE VERIFICATION



PCI DSS



iBeta L3



ISO 27001:2022



CE+



QG GDPR



SOC2



GDPR



CCPA

How commercial gaming is regulated in the UAE

The GCGRA sets and supervises AML/CFT obligations for every Gaming Operator

For an iGaming business already licensed elsewhere and now expanding into the United Arab Emirates, the requirements set out in this guide apply from the point of licensing, so they belong in the market-entry plan rather than after it. The General Commercial Gaming Regulatory Authority (GCGRA) holds exclusive federal jurisdiction over commercial gaming in the United Arab Emirates, and financial crime is a central part of that mandate.

Because the authority sets the AML/CFT standards, supervises compliance with them and investigates breaches within the same remit that governs the wider sector, a Gaming Operator does not answer to one body for its conduct and a separate one for its anti-money-laundering controls. It answers to the GCGRA for both, which establishes financial crime as a licensing matter rather than a parallel obligation.

That AML/CFT basis was made explicit in 2024, when a Ministerial Resolution issued by the UAE Ministry of Finance brought Internet Gaming Operators, Land-Based Gaming Facilities Operators, Sports Wagering Operators and Lottery Operators within the definition of Designated Non-Financial Businesses and Professions (DNFBPs) under Federal Decree Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organizations. The same resolution established the GCGRA's AML/CFT supervisory powers, so those AML/CFT obligations apply to an operator through its gaming licence rather than as a separate requirement.

FIGURE 1

The federal instruments a licensed Gaming Operator answers to

GCGRA Executive Regulations direct licensed Gaming Operators to comply with

Federal Law No. 7 of 2014

Combatting Terrorism Offences

Federal Decree Law No. 20 of 2018, as amended

Anti-money laundering and combating the financing of terrorism

Cabinet Decision No. 10 of 2019

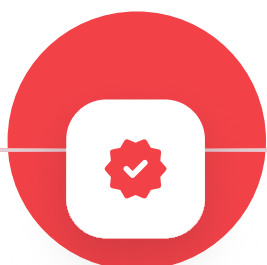
Implementing regulation of Federal Decree Law No. 20 of 2018

Cabinet Decision No. 74 of 2020

Terrorist lists and the implementation of UN Security Council resolutions

The AML/CFT framework is in force now, not a future expectation

Commercial gaming in the UAE already operates under live supervision, so these obligations are current requirements rather than proposals to be addressed at a later stage. The GCGRA has issued the country's first Gaming Operator licences, brought the UAE Lottery under real-time oversight, and established the means to monitor illegal activity, investigate breaches and act against unlicensed operators, so an operator's AML/CFT controls are now assessed by a regulator that is already applying them.



LICENSING

First licences issued

The country's first Gaming Operator licences have been issued.



OVERSIGHT

Real-time oversight

The UAE Lottery has been brought under real-time oversight.



ENFORCEMENT

Action against operators

Means established to monitor illegal activity, investigate breaches and act against unlicensed operators.

The GCGRA AML/CFT framework for Gaming Operators

The AML/CFT framework runs across ten requirement areas

The Commercial Gaming Policy Paper sets out the AML/CFT framework for licensed Gaming Operators across ten requirement areas, which fall into institutional controls, the player journey, detection and reporting, and the evidence and systems that support them.

FIGURE 2

The ten AML/CFT requirement areas, grouped by where they operate

INSTITUTIONAL CONTROLS	Governance and oversight	MLRO appointment
	Institutional risk assessment	
PLAYER JOURNEY	Player risk assessment	Player Due Diligence
	Enhanced Due Diligence	
DETECTION AND REPORTING	Sanctions compliance	Suspicious activity reporting
EVIDENCE AND SYSTEMS	Record keeping	Technical compliance

The table below sets out the requirements an operator must meet at board and infrastructure level, while the requirement areas that operate inside the player journey are examined in the following sections.

Requirements at board and infrastructure level

REQUIREMENT AREA	WHAT THE FRAMEWORK EXPECTS
Governance and oversight	The board oversees AML compliance, policies, procedures and internal controls, and the wider AML/CFT risk management framework.
Institutional risk assessment	The operator assesses the money laundering risk its own business carries across customer types, geographic areas of operation, products and services, distribution channels, transaction volumes and new technologies.
MLRO appointment	An MLRO of suitable seniority, experience and independence, who regularly resides in the UAE and reports on risks, issues and trends to senior management on a semi-annual basis.
Record keeping	Due diligence records, transaction records, internal and external suspicious activity reports, FIU correspondence and risk assessment documentation held for five years after the last transaction or the end of the player relationship.
Technical compliance	An information security management system aligned with ISO/IEC 27001, periodic vulnerability assessment and penetration testing, and product certification by independent testing laboratories.

Supervision begins before a licensee commences operations

Before any licensee may commence operations, the GCGRA conducts a review of its internal controls, including AML and CFT policies, cybersecurity protocols and compliance frameworks, in order to assess operational readiness. Once operations begin, supervision runs on a risk-calibrated basis that may include periodic inspections, data reviews, thematic audits and third-party independent assessments mandated by the authority, with the frequency and intensity of that activity determined by business scale, transaction volume, technology footprint and prior compliance history.

The review examines controls that are already operational, so player verification, screening and monitoring must be in place and evidenced by the time an operator reaches it. Compliance history then informs the risk calibration that follows, which works in favour of an operator able to demonstrate a clean record in the markets where it already holds a licence.



Periodic inspections

Supervision runs on a risk-calibrated basis once operations begin.



Data reviews and thematic audits

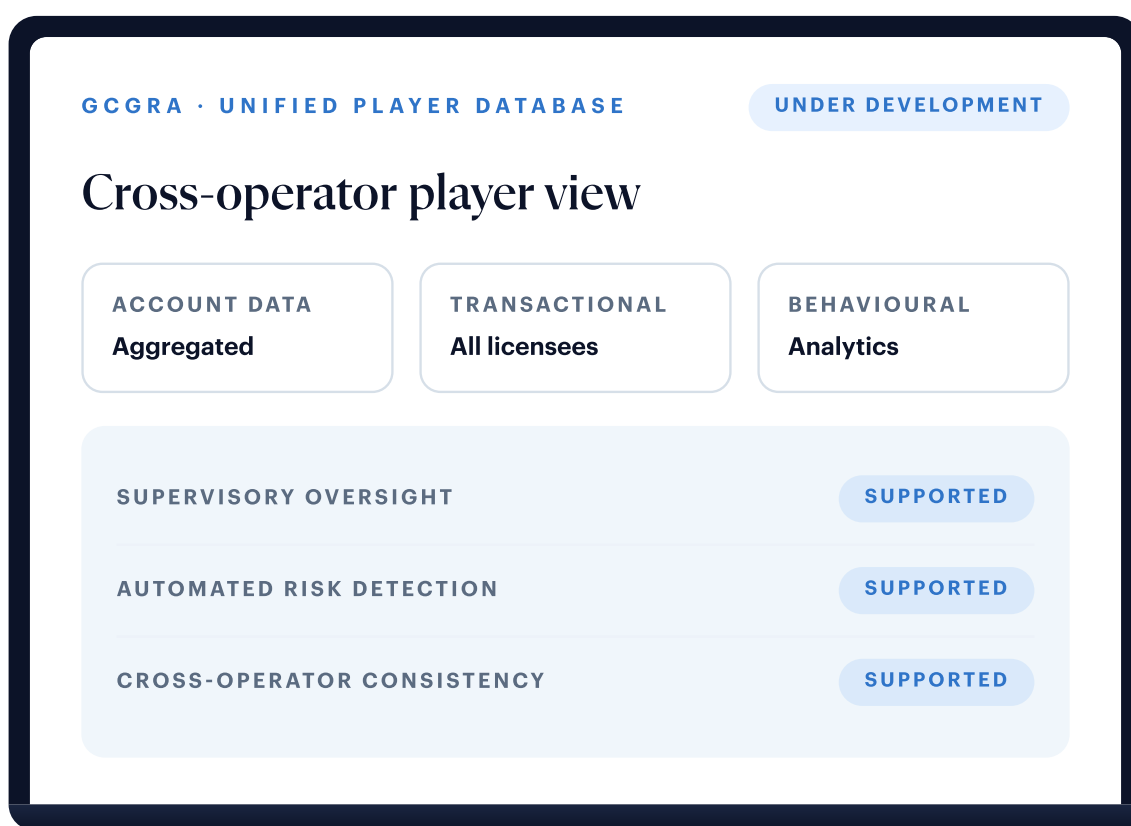
Frequency and intensity are set by business scale, transaction volume, technology footprint and prior compliance history.



Third-party independent assessments

Mandated by the authority.

The Unified Player Database will give the regulator a cross-operator view



The GCGRA is developing a Unified Player Database (UPDB), a centralised platform that will aggregate player account information, transactional data and behavioural analytics across all licensees, in order to support supervisory oversight, automated risk detection and cross-operator consistency. Under that model, player-level data quality is no longer a purely internal concern, because the record an operator holds on a player becomes the record a supervisor can compare against every other licensee's view of the same person.

Player Due Diligence

Four obligations that build on one another, and the account threshold at which they apply.

Four Player Due Diligence obligations and one account threshold

Player Due Diligence in the UAE rests on four obligations that build on one another rather than operating independently. An operator must verify each player's identity independently and reliably, establish and assess the relationship it is entering into with that player, assess the risk profile the player presents, and then monitor play in real time against the information it already holds.

The order matters, because each obligation depends on the record produced by the previous one, and the point at which these obligations apply is the Player Account: once linked deposits and withdrawals cumulatively exceed AED 11,000, the activity must run through a Player Account and Player Due Diligence applies to it.

FIGURE 3

The four Player Due Diligence obligations and the AED 11,000 Player Account threshold





PLAYER ACCOUNT THRESHOLD

AED 11,000

THE POINT AT WHICH PLAYER DUE DILIGENCE APPLIES

The point at which these obligations apply is the Player Account: once linked deposits and withdrawals cumulatively exceed AED 11,000, the activity must run through a Player Account and Player Due Diligence applies to it.

FATF RECOMMENDATION 22

The account-based structure

The account-based structure the UAE has adopted follows the international standard written for this sector. Under FATF Recommendation 22, casinos, which the FATF standards define to include internet casinos, are DNFBPs that must apply customer due diligence once a customer's financial transactions reach or exceed the designated threshold of USD or EUR 3,000, whether in a single operation or in several operations that appear to be linked.

THE INTERNATIONAL STANDARD

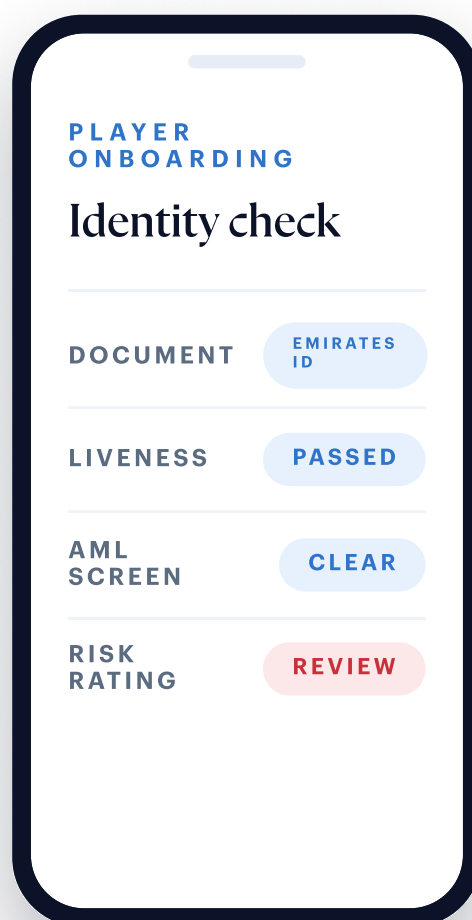
The measures this designation brings with it are those a bank already applies, because Recommendation 22 extends the customer due diligence and record-keeping obligations of Recommendations 10, 11, 12, 15 and 17 to casinos: identity verification, record keeping, politically exposed person checks, attention to the risks of new technologies, and controls over any reliance on third parties all apply to a gaming operator as they do to a financial institution.

The interpretive note to Recommendation 22 goes further, since a country must have its casinos link the customer due diligence information they hold on a player to the transactions that player conducts, which is the function a Player Account performs. The GCCRA Executive Regulations carry provisions aligned with Recommendation 22, and the UAE has set its own dirham figure for that linked-transaction test.

The right KYC solution for Player Due Diligence

For an iGaming operator, Player Due Diligence is primarily a procurement decision, because the four obligations above are only as effective as the KYC solution selected to deliver them. Three criteria separate a solution suited to a UAE gaming product from one that is not.

Firstly, it must provide broad document coverage, because a UAE-facing product onboards residents and visitors holding travel and identity documents issued across a wide range of countries, and a solution limited to a narrow document set will reject genuine players rather than fraudulent ones.



PLAYER ONBOARDING

Identity check

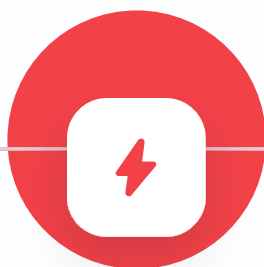
DOCUMENT	EMIRATES ID
LIVENESS	PASSED
AML SCREEN	CLEAR
RISK RATING	REVIEW



FIRSTLY

Broad document coverage

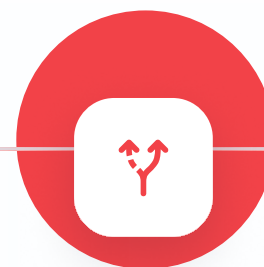
A UAE-facing product onboards residents and visitors holding travel and identity documents issued across a wide range of countries.



SECONDLY

Verification at product pace

A player who abandons onboarding during document capture is a lost customer.



THIRDLY

A route for thin footprints

A non-documentary or step-up path which verifies these players rather than rejecting them.

Secondly, it must complete verification at the pace a live product demands, since a player who abandons onboarding during document capture is a lost customer, frequently to a competitor or to an unlicensed offshore operator of the kind the GCGRA acts against. Thirdly, it must offer a route for players with a limited documentary footprint, the case the policy paper highlights when it notes the difficulty of verifying identity, establishing source of wealth and assessing risk profiles for foreign players based in higher-risk jurisdictions. In practice, that means a non-documentary or step-up path which verifies these players rather than rejecting them.

Player risk assessment and Enhanced Due Diligence

When a player is risk-rated, and on what basis

A player's risk rating is not a fixed classification assigned once at onboarding. The framework expects the risk rating to be assigned when the account is created, revisited periodically thereafter, and reopened whenever a risk factor changes, so the rating an operator holds is intended to reflect the player throughout the relationship rather than only at account opening.

FIGURE 4

The three points at which a player risk rating is assigned or revisited



A change in risk factors returns the player to assessment.

The risk rating is held on file and has to be evidenced later.

How the risk rating is determined is left to the operator. The policy paper accepts that several approaches are workable depending on an operator's nature, size and complexity, and it identifies data-driven dynamic risk-rating models that score transactional behaviour and other attributes close to real time as one approach an operator may adopt.

It also provides a worked example of a change in risk factors, proposing that **a player who begins using several payment instruments should prompt a review of that player's risk rating.**

What Enhanced Due Diligence covers

Enhanced Due Diligence is the more rigorous set of checks an operator applies when standard Player Due Diligence is not sufficient to manage a player's risk. It applies by default to two groups, politically exposed persons and players the operator has already rated high risk, and for those players it adds further measures on top of ordinary Player Due Diligence rather than replacing it.

FIGURE 5

Enhanced Due Diligence, who it applies to and what it includes

WHAT ENHANCED DUE DILIGENCE INCLUDES

- | | | | |
|---|--|---|---|
| 1 | Additional identity information, including intended use of the account | 2 | More frequent updates to due diligence data |
| 3 | Source of funds and source of wealth | 4 | Tighter scrutiny of accounts and transactions |
| 5 | Senior management approval before opening or transacting | 6 | Systems to identify and monitor PEPs |
| 7 | Increased vigilance over ongoing account activity | | |

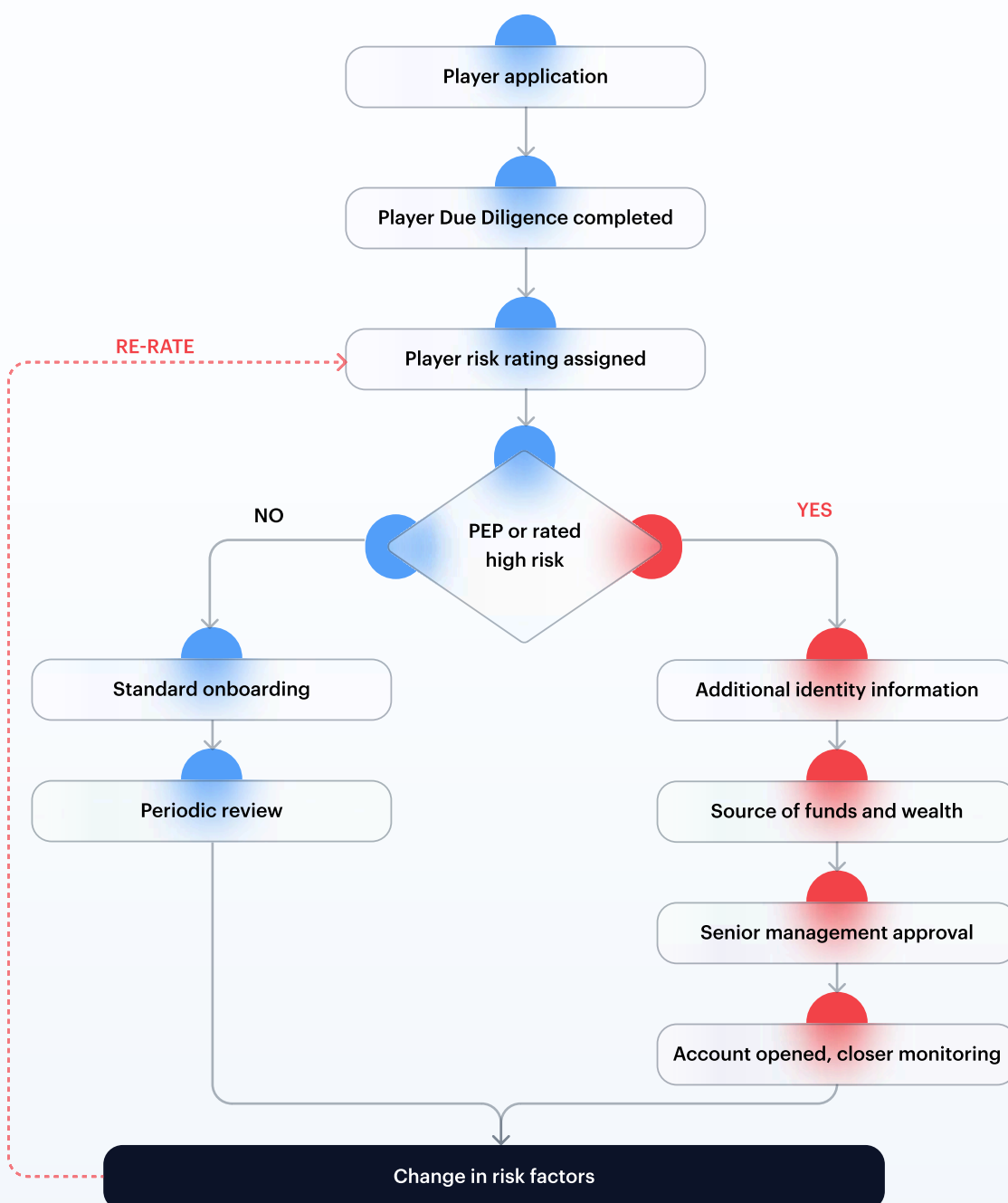
How Enhanced Due Diligence applies to players' verification across the UAE

For players subject to Enhanced Due Diligence, verification is no longer a single onboarding step but a sequence the operator completes before the account is permitted to transact freely, as set out in the flow below. Because the UAE onboards players from many nationalities and residency situations, that sequence must accommodate identity documents issued across a wide range of countries and formats, and it must produce a record the operator can retrieve months later, since the decision and its supporting evidence are subject to supervisory examination.

These players also remain under closer ongoing monitoring for the life of the account, more frequent than the periodic review applied to a standard player.

FIGURE 6

The Enhanced Due Diligence decision path from application to ongoing monitoring



The Enhanced Due Diligence decision path from application to ongoing monitoring

When Enhanced Due Diligence is required

To ensure the appropriate level of Enhanced Due Diligence for players in the UAE iGaming sector, two triggers apply automatically, and the remaining considerations are left to the operator's judgement. Enhanced Due Diligence applies whenever a player is a politically exposed person or has been rated high risk, and neither case is discretionary, so an operator that identifies either must place the player on the enhanced path.

Beyond these two, the policy paper sets out international best practice drawn from other jurisdictions, which it presents as measures to consider following a sectoral risk assessment rather than as fixed UAE requirements.

On that basis, the paper recommends Enhanced Due Diligence in three further situations.



FIRSTLY

High-value customers

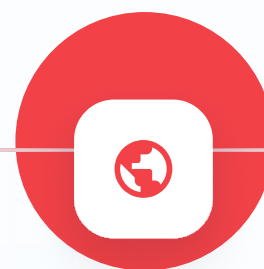
Paired with source-of-funds and source-of-wealth checks.



SECONDLY

Third-party payments

Above a defined threshold, where the funds reaching an account are not evidently the player's own.



THIRDLY

Higher-risk jurisdictions

Players and transactions connected to higher-risk jurisdictions, where the geographic exposure is greater.

The operator's decision is therefore not whether to apply Enhanced Due Diligence, but how broadly to define the population subject to it, since that definition determines the operational load it creates.

Choosing the right Identity Verification and Risk Assessment Partner for UAE Market

A vendor assessment checklist for UAE gaming compliance

WHAT TO ASSESS

THE QUESTION TO ASK THE VENDOR

Document verification

Can it authenticate identity documents, the Emirates ID included, across the full range of nationalities you onboard, not only a narrow Western set?

OCR extraction and form pre-fill

Does it use OCR to extract identity data from the document and pre-fill the onboarding form, so a player does not re-enter details the document already contains?

Non-documentary (eIDV) verification

Does it offer non-documentary verification through UAE Pass and authoritative government sources, available to any player rather than only as a fallback for those without a document?

Biometric liveness

Can it confirm a live person and detect deepfake and presentation attacks at the point of capture?

AML screening

Does it screen everyone onboarded against sanctions, PEP, watchlist and adverse-media data, with match thresholds you can tune?

Source-of-funds evidence

Can it collect and review source-of-funds and source-of-wealth documents inside the Enhanced Due Diligence flow, and leave an audit-ready record?

WHAT TO ASSESS**THE QUESTION TO ASK THE VENDOR**

Ongoing monitoring

Does screening keep running after onboarding and re-check an account when its holder's status changes?

Risk-rating support

Does it provide structured, current data your risk-rating model can query, rather than static documents in a file?

Multi-Accounting and Bonus Abuse Prevention

Can it link identities and devices across accounts to catch multi-accounting and bonus or promotion abuse before a payout?

Record keeping

Does every decision leave an evidence pack you can retrieve and produce to the GCGRA across the five-year retention window?

Data residency and deployment

Can it be deployed to meet UAE data-residency expectations, whether cloud, local cloud, on-premises or hybrid?

Speed

Does identity verification complete at the pace a live gaming product needs, so that neither document capture nor the overall verification process is where sign-ups are lost?

How Shufti supports UAE KYC, AML and fraud prevention

The checklist sets out what a UAE gaming operator needs from a verification partner, and Shufti's platform addresses it from a single API.



Document verification

Government-issued IDs from 240+ countries and territories, with forensic checks on security features, the machine-readable zone and, where present, the NFC chip.



OCR and form pre-fill

OCR trained natively on 150+ languages including Arabic extracts the document data and pre-fills the onboarding form, so a player retypes nothing.



Docless verification flows

A first-class onboarding path rather than a fallback, run through eIDV: 30+ national eID schemes including UAE Pass, plus authoritative government databases, in under three seconds. Only low-confidence results step up to document or video verification.



Biometric liveness

Confirms a live person and detects deepfake and presentation attacks at capture, with iBeta Level 3 conformance.



AML screening

Sanctions, including OFAC, the EU consolidated list, UK HMT and the UN, plus 1,200+ PEP databases and adverse media in 80+ languages. Thresholds are tunable and screening continues after onboarding.



Source of funds and wealth

Collected and reviewed inside the Enhanced Due Diligence flow, with configurable MLRO-backed review and an audit-ready record.



Multi-Accounting and Bonus Abuse Prevention

Device fingerprinting and shared-device signals link identities across accounts before a bonus is paid.

240+

Countries and territories covered for government-issued document verification.

30+

National eID schemes including UAE Pass, verified in under three seconds.

REFERENCES

-
- 1 General Commercial Gaming Regulatory Authority and NAMLCFTC, Commercial Gaming Policy Paper (2025). Primary regulatory basis.
 - 2 FATF, The FATF Recommendations, Recommendation 22 on DNFBPs and its interpretive note. [fatf-gafi.org](https://www.fatf-gafi.org)
 - 3 General Commercial Gaming Regulatory Authority. gcgra.gov.ae
 - 4 Shufti product and coverage pages for document verification, electronic identity verification, AML screening and fraud prevention. shuftipro.com
-

Sources accessed September 2026.



Building a Stronger Player Verification Framework

To see how these journeys apply to your own onboarding requirements,
book a Shufti demo for the UAE market.

[Request a Demo](#)

Shufti is based in the United Kingdom and operates offices worldwide.



United States

16200 SW Pacific Hwy,
Suite H PMB 1053,
Tigard, OR



Cyprus

Arch. Makarios III
Avenue 229, Limassol



Dubai

Unit 507, Level 5, Gate
District Precinct
Building 03, DIFC,
Dubai



Hong Kong

8 Queen's Road East,
Wan Chai, Hong Kong



Pakistan

322-G3 Main Blvd,
Johar Town, Lahore,
Pakistan



Singapore

68 Circular Road
#02-01, Singapore



United Kingdom

Office 408,
Coppergate House, 10
Whites Row, London
E1 7NF

shuftipro.com
sales@shuftipro.com