Shufti

Brazil

GUIDE

Brazil Bets KYC Playbook

SPA/MF-Ready Identity Verification for Licensed .bet.br Operators

VÉRIFICATION D'ÂGE KJM

PCI DSS

iBeta Niveau 1

ISO 27001: 2013

CE+

QG GDPR

SOC2

GDPR

CCPA

Executive Summary

Brazil's licensed betting market has moved from licensing-phase oversight into active operational compliance enforcement. For .bet.br operators, the question is no longer whether to implement KYC controls. It is whether what was built for initial licensing still holds up under enforcement scrutiny.

SPA/MF compliance now requires a connected identity workflow spanning nine separately audited controls: CPF validation, document verification, certified biometric liveness, age assurance, AML and PEP screening, SIGAP self-exclusion integration, LGPD biometric consent management, automated re-verification, and structured audit trail export. Each has its own regulatory source. Each can generate an independent compliance finding. Failing one layer creates operator liability even where the remaining eight are fully compliant.

This guide maps the full control environment and gives compliance, risk, fraud, and operations teams the tools to audit, remediate, and implement: a regulatory control map, a step-by-step operating model with audit evidence requirements for each control, a vendor evaluation framework with RFP questions, an implementation roadmap, and a pre-enforcement audit checklist.

Who Should Read This Guide

This guide is for compliance officers, MLROs, fraud leaders, product owners, and operations teams at licensed .bet.br operators. Also relevant for technology and legal teams evaluating KYC vendor capability against SPA/MF requirements.

Shufti

Table of Contents

Brazil betting market · 2025

BRL 36.96bn

in gross gaming revenue across 25.2 million active bettors. LATAM's largest regulated betting market, with 173+ licensed operators.

Why Brazil Bets KYC Is Different

Brazil's betting market generated BRL 36.96 billion in gross gaming revenue across 25.2 million bettors in 2025, making it the fifth-largest globally and LATAM's largest regulated betting market, with 173+ licensed operators. The scale of the market is matched by the rigour of its regulatory framework.

What Changed

In 2025, Brazil's Secretaria de Premios e Apostas (SPA) moved from licensing oversight into active compliance monitoring. In May 2025, SPA suspended seven operators for cybersecurity non-compliance, with daily fines of R$40,000 per violation. Brazil's enforcement posture is now expanding beyond initial licensing and cybersecurity documentation into broader operational controls. Operators should expect identity verification, AML reporting, self-exclusion workflows, biometric certification, and audit trail availability to become active inspection priorities as SPA/MF matures its oversight model.

This matters because enforcement tests whether policies are actually enforced in production logs, not whether they are documented in a compliance manual. The gap between what was built for licensing approval and what SPA now inspects is where exposure sits.

R$40,000/day

per violation. SPA suspended seven operators for non-compliance. Brazil's enforcement posture is expanding beyond licensing into live operational controls.

Why Most Operators Are Exposed

Most .bet.br operators built their KYC flows for initial licensing approval, not for ongoing enforcement scrutiny. The gaps are predictable: document verification trained on limited RG formats, liveness detection that is not certified against recognised PAD standards, self-exclusion checks that are manual rather than automated, AML screening that runs at registration but not continuously, and biometric consent bundled into Terms of Service rather than captured as a standalone record. Each gap is a potential enforcement finding.

Three Structural KYC Challenges

1. Regulatory Integration: No Single Check Is Sufficient

SPA/MF requires CPF, document, liveness, AML, self-exclusion, age assurance, biometric consent, re-verification, and audit trail as a connected system. Each layer is individually mandated and individually audited. Failing one layer creates operator liability even if the remaining layers are fully compliant.

2. Document Complexity: 27 State-Level Formats With No Federal Standard

Brazil's primary national identity document, the Registro Geral (RG), is issued by state governments with no federal standardisation. Brazil has 27 states, each with distinct RG formats, numbering schemes, and security features. Operators whose document verification vendors are trained on a narrow document set face materially higher false rejection rates, user abandonment, and manual review backlogs.

3. Enforcement Maturity: From Licensing Into Active Inspection

Brazil is no longer in the licensing phase. SPA is now auditing live operator flows against operational compliance criteria. Operators who passed licensing with documented policies must now demonstrate that those policies are enforced in production data, visible in structured audit logs, and verifiable on request.

For compliance, risk, fraud, and operations teams, Brazil's KYC regime requires a vendor stack that covers the full control map, not a selection of isolated checks.

For compliance, risk, fraud, and operations teams, Brazil's KYC regime requires a vendor stack that covers the full control map, not a selection of isolated checks.

The Brazil Bets Regulatory Control Map

Five primary ordinances and two national laws define the compliance control environment for licensed .bet.br operators. The visual below maps each control to its regulatory source, operational requirement, operator risk, and system ownership.

CPF Validation	Portaria 722/1,143	IDENTITY
Document Verification	Portaria 722/1,231	IDENTITY
Biometric Liveness	Portaria 722	IDENTITY
Age Assurance	Lei 14.790/Lei 15.211	IDENTITY
AML / PEP Screening	Portaria 1,143	AML
Self-Exclusion / SIGAP	Instruction No. 31	PLATFORM
Biometric Consent (LGPD)	Lei 13.709/2018	PRIVACY
Re-Authentication	Portaria 722	PLATFORM
Audit Trail	Portaria 722 Art. 25	ALL CONTROLS

The CPF Is an Eligibility Gate, Not an Identity Control

For Brazil .bet.br operators, CPF validation is the first eligibility gate: it confirms a bettor exists in the Receita Federal database and is not deceased or suspended. It is not an identity assurance control. Identity assurance begins only when CPF, document verification, face match, liveness detection, AML screening, and self-exclusion checks are connected in a single verified workflow.

Brazil's Identity Layer: CPF, RG, CNH, CIN

Brazil's identity document system comprises four primary documents, each with distinct regulatory requirements, population coverage, and fraud profiles. Operators must handle all four, not just the newest.

CPF: Cadastro de Pessoas Físicas

The CPF is Brazil's individual taxpayer registration number, formatted as XXX.XXX.XXX-XX across 11 digits. CPF validation under Portaria 722 requires: (1) format validity via modulo-11 syntax check; (2) real-person status against the Receita Federal database; (3) exact name matching to tax records with zero typo tolerance.

What CPF validation catches: Invalid formats, deceased or suspended taxpayer records, name mismatches.

What CPF validation does not catch: Synthetic identity fraud, mule accounts (contas laranja), and credential stuffing from breached databases. Large-scale Brazilian data breaches have exposed CPF numbers at the population scale, making CPF alone an eligibility gate rather than an identity assurance control.

Mule Account Gap: The 3-Step Attack Flow

①

Fraudster buys valid CPF

A real, active CPF number — purchased from an underground data marketplace. Tax record is live. Name is real.

②

CPF validation passes

Account registered with fabricated contact details. CPF is syntactically valid. Receita Federal status: active. Name match: clears. No further checks.

③

Account activated. Fraud begins.

Mule account used for layering, bonus abuse, or payment receipt. No document. No face. No liveness.

The Fix

CPF Validation → Confirms the person exists

Document Verification → Confirms the document belongs to them

Biometric Liveness → Confirms they are physically present

All three together close the gap CPF alone leaves open.

RG: Registro Geral

The RG is issued by state governments with no federal standardisation. Brazil's 27 states each maintain their own RG format, numbering scheme, font conventions, and security features. RG documents produce an estimated 45-55% document verification pass rate, the lowest among accepted Brazilian ID types, primarily due to format variation, photograph aging (10-year validity standardised by federal law in 2022), and security feature degradation.

CNH: Carteira Nacional de Habilitação

The CNH is Brazil's national driver's licence, issued by state traffic authorities (DETRAN). Unlike the RG, the CNH carries standardised national security features. CNH document verification pass rates are materially higher than RG due to its standardised national format. The limitation is that not all Brazilians hold a driver's licence.

CIN: Carteira de Identidade Nacional

The CIN is Brazil's federal-standard identity card designed to replace the fragmented RG system. It integrates fingerprints, facial biometrics, and CPF as a single identifier. As of early 2025, 20 million Brazilians had received a CIN, with the government targeting 130 million issued by end-2026. Expected document verification pass rates exceed 80-90%.

The transition problem: Operators cannot design KYC flows for CIN alone. Brazil will remain a mixed-document environment for years. KYC flows must simultaneously support legacy RG across all 27 state formats, CNH, passport, and the accelerating CIN rollout.

CPF

Cadastro de Pessoas Físicas

Issuer: Federal (Receita Federal)

Coverage: 100%

Pass Rate: N/A

HIGH Eligibility gate only

RG

Registro Geral

Issuer: 27 state formats

Coverage: ~90%

Pass Rate: 45-55%

HIGH Highest rejection

CNH

Carteira Nacional de Habilitação

Issuer: State (DETRAN)

Coverage: ~40%

Pass Rate: 75-85%

MEDIUM Standardized format

CIN

Carteira de Identidade Nacional

Issuer: Federal standard

Coverage: ~15% (growing)

Pass Rate: 80-90%

LOW Preferred option

The Brazil Bets KYC Operating Model

The nine steps below map directly to the SPA/MF ordinances identified in the Regulatory Control Map. Each step identifies its regulatory source, operational requirement, vendor capability needed, and the audit evidence that must be available if regulators request it.

PORTARIA 722/2024 -- STEP 1

CPF Validation

What It Requires

Portaria 722 requires real-time CPF validation during onboarding. Portaria 1,143 mandates CPF validation before account activation. Validation must confirm: (1) modulo-11 format validity; (2) active status in the Receita Federal database; (3) exact name matching with zero typo tolerance.

What Your Vendor Must Do

- Real-time API integration with the Receita Federal database
- Exact name-matching with zero tolerance for mismatches
- Flagging of suspended, cancelled, or deceased CPF status

Audit Evidence Required

- CPF validation result, timestamp, actor ID
- CPF status at time of validation (active, suspended, cancelled)
- Name-match outcome and tolerance applied
- Retry log if re-attempt was triggered

PORTARIA 722/2024 -- STEP 2

Document Verification Across Brazilian ID Variants

What It Requires

Document verification must handle the full Brazilian identity document ecosystem: all 27 RG state format variations, CNH, CIN, and passport. The structural challenge is RG: operators cannot use a vendor trained on a single state's format and expect compliant pass rates for a nationally distributed user base.

What Your Vendor Must Do

- Zero-configuration support for all 27 RG state format variants
- Multi-level security feature detection: holograms, barcodes, laminates, watermarks
- Photograph age tolerance to handle photos up to 10 years old without false rejection (RG validity standardised at 10 years since 2022)
- CIN rollout support alongside legacy documents
- Human review escalation for borderline cases with full audit logging

Audit Evidence Required

- Document type, issuing state (for RG), document number
- Security feature check results and confidence score
- Verification outcome (accepted, rejected, escalated), timestamp, actor ID
- Image capture quality score
- Retry or escalation log if applicable

PORTARIA 722/2024 -- STEP 3

Biometric Liveness Detection

What It Requires

Portaria 722 explicitly prohibits static selfies. Operators must deploy liveness detection certified against recognised presentation attack detection standards, such as ISO/IEC 30107-3 or iBeta PAD Level 1/2, and validated by a SPA-recognised testing body. SPA recognises five testing bodies: Gaming Laboratories International LLC, Trisigma BV, Quinel Limited, eCOGRA Limited, and BMM North America Inc.

What Your Vendor Must Do

- Certification against recognised PAD standards from a SPA-recognised testing body
- Active and/or passive liveness options
- Deepfake and synthetic face detection (silicone masks, face-swap attacks)
- Confirmed currency of certification: the specific algorithm version in production must be covered

Audit Evidence Required

- Certification document: body, level, date, algorithm version covered
- Liveness result (pass/fail), liveness score, presentation attack indicator
- Face-match result and confidence score
- Timestamp, user ID, device/session metadata
- Retry outcome if a re-attempt was triggered

PORTARIA 722/2024 -- STEP 4

The 7-Day Re-Verification Cycle

What It Requires

Portaria 722 mandates multi-factor authentication at least once every 7 days, or upon first access after 7+ days of inactivity. Operators must also re-authenticate users after 30 minutes of device inactivity, with no bets or financial transactions permitted until re-authentication is complete.

What Your Vendor Must Do

- Configurable re-verification triggers: days since last authentication, inactivity duration, transaction type
- Support for SMS/email OTP, TOTP, biometric step-up, and push notification re-auth
- Automated enforcement via system logic, not manual review

Audit Evidence Required

- Re-verification trigger type (7-day cycle or 30-min inactivity)
- Authentication method used, outcome, and timestamp
- User ID, device ID, session metadata
- Monthly log confirming enforcement across all active accounts

LEI 15.211/2025 -- STEP 5

Age Assurance

What It Requires

Lei 14.790/2023 sets a hard minimum age of 18 for Brazilian betting platforms. Lei 15.211/2025, a digital child safety law effective March 17, 2026, applies to online platforms, including licensed betting operators. It raises the standard beyond self-declaration or checkbox-only age gates, requiring reliable and auditable age-assurance mechanisms. Compliance officers should confirm with their legal team how Lei 15.211 applies to their specific operator structure.

What Your Vendor Must Do

- Document date-of-birth extraction and cross-referencing against CPF age data
- Biometric face-match to verify that the person presenting the document matches the document holder
- Age-assurance audit log: what evidence was used, what outcome was reached, and timestamp

Audit Evidence Required

- Age-assurance method used (document DOB, CPF cross-reference, face match)
- Result and timestamp
- Document type used for age verification
- Outcome: approved, rejected, escalated for review

REGULATORY INSTRUCTION NO. 31 -- STEP 6

SIGAP and Self-Exclusion Compliance

What It Requires

SIGAP (Sistema de Gestão de Apostas) is Brazil's centralised government betting management system, launched in December 2025. Regulatory Instruction No. 31 mandates SIGAP integration with specific query requirements: at account registration, at first daily login, and every 15 days for all active users. If a user appears on the self-exclusion register, operators must block access and return the user's balance within 72 hours of receiving the notification.

What Your Vendor Must Do

- Native SIGAP API integration or documented integration pathway
- Automated account blocking upon self-exclusion notification, with no manual steps in the critical path
- Balance return workflow with timestamp logging
- Scheduled query automation: daily first-login checks and 15-day recurring checks

Audit Evidence Required

- SIGAP query timestamp and result (matched / not matched)
- Self-exclusion notification receipt timestamp (if applicable)
- Account blocking action timestamp and actor ID
- Balance return timestamp and amount (if applicable)
- Scheduled query log confirming 15-day cycle compliance

PORTARIA 1,143/2024 -- STEP 7

PEP, Sanctions, and AML Screening

What It Requires

Portaria 1,143/2024 mandates screening all bettors for PEP status and sanctions list membership as a continuous obligation. PEP status changes over time. Reporting to COAF via SISCOAF is mandatory for all suspected terrorism financing. Under Portaria 1,143, reporting is risk-based rather than threshold-based: operators must report any transaction that raises AML or CFT suspicion, regardless of amount.

What Your Vendor Must Do

- PEP list coverage: Brazilian domestic PEP definitions and international FATF-standard PEP lists
- Sanctions list coverage: 1,000+ sources minimum
- Continuous screening with frequent list refresh (daily or more frequent)
- SISCOAF-compatible reporting output

Audit Evidence Required

- PEP/sanctions check result, list version used, timestamp, user ID
- Match details if a match was returned (match type, source list)
- Risk tier assigned and review outcome if escalated
- SISCOAF report reference number if a report was filed
- Continuous screening log confirming schedule compliance

LGPD -- LEI 13.709/2018 -- STEP 8

LGPD Compliance for Biometric Data

What It Requires

Brazil's Lei 13.709/2018 (LGPD) classifies biometric data as sensitive personal data requiring explicit, separate consent. ANPD enforces LGPD with fines reaching 2% of annual revenue per violation (maximum R$50 million). Consent records must capture: date, timestamp, form version, purpose, and IP address.

What Your Vendor Must Do

- Standalone consent flow, separate from ToS acceptance
- Purpose-specific consent language for biometric data collection
- Withdrawal mechanism: users must be able to withdraw biometric consent
- Consent audit log with timestamp, form version, IP address, and retention period
- Minimum 5-year consent record retention

Audit Evidence Required

- Consent record: date, timestamp, form version, purpose statement, IP address
- Consent withdrawal record (if applicable)
- Data retention period confirmed for biometric data held
- The LGPD data processing basis is documented for each biometric data type

PORTARIA 722/2024 -- STEP 9

Building the Regulator-Ready Audit Trail

What It Requires

Portaria 722 mandates audit trails covering all operations and user activity with a minimum 36-month retention period per Portaria 722 Article 25, covering account statements and transaction logs. Operators with AML obligations should confirm with legal counsel whether longer retention applies under COAF guidance. Exports are required in XML, XLS, and CSV formats. Daily and monthly submissions to SPA via SIGAP are required.

What Your Vendor Must Do

- Structured audit exports in XML, XLS, and CSV formats
- Granular event logging: timestamp (ISO 8601), actor ID, action type, result, and supporting evidence
- 5-year redundant backup storage
- SIGAP-compatible daily and monthly submission capability

Audit Evidence Required

- Full user verification timeline: CPF result, document result, liveness result, AML result, SIGAP result, consent record, and final account activation decision in one exportable record
- Timestamp (ISO 8601), actor ID, action type, and result for every KYC event
- Backup storage confirmation with redundancy documentation
- Sample XML, XLS, and CSV exports for regulator review

Where .bet.br Operators Fail

Enforcement actions and compliance audits have revealed six recurring failure patterns across licensed operators. Each represents a gap between initial licensing approval and operational compliance under active enforcement scrutiny.

Failure Point 1: Ghost Accounts: No Biometric Liveness

Problem: Operators activate accounts using valid CPFs without biometric liveness verification. Fraudsters create synthetic identities using real CPFs combined with fabricated supporting details. Without certified liveness detection, these accounts pass registration.

Regulator Risk: Non-certified or absent biometric liveness is a direct Portaria 722 violation. Ghost accounts created through this gap represent one of the primary compliance risks SPA's active monitoring is designed to detect.

Fix: Mandate certified biometric liveness before account activation, with no exceptions. Every registration must complete CPF validation, document verification, and certified liveness before any account is activated, bets are placed, or deposits are accepted.

Failure Point 2: Document Verification Failure Rate Creating Abandonment

Problem: Operators partner with document verification vendors that handle only a subset of Brazilian RG state formats. RG false rejection rates reach 60%+ for legitimate users. Users fail verification, retry, fail again, and abandon the registration flow.

Regulator Risk: High false rejection rates create two simultaneous risks: user abandonment that directly impacts first-deposit conversion, and manual review backlogs that create compliance gaps.

Fix: Partner with a multi-format-trained document verification vendor covering all 27 RG state variants. Accept multiple document types (RG, CNH, CIN) so that users whose RG fails can proceed with an alternative.

Failure Point 3: SIGAP Blocking Not Automated Within 72 Hours

Problem: Operators receive SIGAP self-exclusion notifications but route them through a manual review queue. The bettor places bets over several days before the operator's manual process triggers account blocking.

Regulator Risk: Potential penalties under Brazil's betting enforcement framework can reach up to 20% of revenue, depending on the violation and enforcement basis. The 72-hour deadline is measured from notification receipt, not from the operator's manual review decision.

Fix: Automate SIGAP blocking as a system-level action with no human approval in the critical path. Set an internal target of 24-hour blocking to provide a compliance buffer against the 72-hour regulatory deadline.

Failure Point 4: 7-Day Re-Verification Rule Not Consistently Enforced

Problem: Operators implement 7-day re-verification in documentation but enforce it inconsistently in production, typically only triggering re-auth on withdrawal requests. Users bet continuously for 30+ days without re-authentication.

Regulator Risk: Portaria 722 non-compliance. A compliance audit that checks re-verification logs will find gaps between documented policy and actual enforcement.

Fix: Enforce 7-day re-verification via automated system logic, not manual check or periodic batch review. Log every re-verification attempt and outcome.

Failure Point 5: AML Screening Run at Registration Only

Problem: Operators screen bettors at account opening and treat this as permanent clearance. PEP status changes over time. A bettor who was clean at registration may acquire a PEP designation months later without the operator's awareness.

Regulator Risk: Portaria 1,143/2024 requires continuous screening. An operator whose screening policy is registration-only is non-compliant with an ongoing AML obligation.

Fix: Implement continuous PEP and sanctions screening with automated list refresh on a daily or more frequent cycle.

Failure Point 6: Weak Audit Evidence: Checks Done, Proof Missing

Problem: Operator completes KYC checks but cannot reconstruct the decision trail during a regulator audit. Screenshots, fragmented platform logs, and vendor dashboards are not structured audit evidence.

Regulator Risk: Portaria 722 mandates structured audit trail exports in XML, XLS, and CSV formats with granular event detail. An operator that cannot produce a full user verification timeline on request faces a compliance finding even if its underlying checks were correctly performed.

Fix: Build a single audit trail that records timestamp, user ID, vendor result, decision outcome, and reviewer action for every KYC event. Test XML, XLS, and CSV exports before an audit request arrives.

What a Compliance Review Should Confirm: Before your next SPA enforcement cycle, your audit trail should be able to answer:

(1) Was every account activated only after CPF, document verification, and certified liveness were all completed?
(2) Has every active user re-verified within the last 7 days?
(3) Has every SIGAP notification resulted in account blocking within 72 hours?
(4) Has every bettor been screened for PEP/sanctions status as of the most recent list refresh?
(5) Can you export a full user verification timeline in XML, XLS, and CSV formats on demand? If you cannot answer yes to all five, you have compliance gaps before you have an enforcement problem.

Operators who want to benchmark their current KYC setup against these six failure patterns can review Shufti's Brazil KYC coverage and capability stack before the next enforcement cycle.

Compliance vs Conversion: Reducing Friction Without Weakening Controls

Brazil .bet.br operators face both compliance and conversion challenges. The goal is to minimise user friction while maintaining full regulatory compliance.

Risk	Compliance Control	Conversion Risk	Best-Practice Fix	Shufti Capability
Leaked CPF / mule account	CPF validation + certified liveness	An additional onboarding step raises abandonment	Use passive liveness: no visible action required; friction-neutral for legitimate users	Active and passive liveness; PAD-certified
RG format variation	Multi-format document verification	False rejection causes retry loops; users abandon	Accept multiple document types (RG, CNH, CIN); offer one retry with a different document type	All 27 RG formats + CNH, CIN, passport; zero-configuration
Self-excluded user	SIGAP query at registration and login	Query latency delays login for clean users	Cache compliant queries with defined TTL; automate blocking; minimise query response time	SIGAP integration support; automated blocking logic
Underage user	Age assurance: document DOB + face match	Youth false positives block legitimate 18+ users	Combine CPF age data + document DOB extraction + biometric face match; provide a clear retry path	CPF + document + face match in single flow
PEP or sanctions match	Continuous AML/PEP screening	Manual review delays account activation	Risk-tier queue: auto-approve low-risk profiles; escalate only confirmed or high-risk matches	1,700+ sources; 20M+ records; updates every 15 min
7-day re-verification trigger	MFA steps up every 7 days	Interrupts active sessions; session abandonment	Use passive biometric step-up where possible; minimise visible friction for returning users	Behavioural biometrics + adaptive MFA step-up

High registration friction	Full KYC stack required before activation	Multi-step flow creates abandonment risk	Use progressive UX, not progressive compliance: keep all required checks before account activation, but reduce friction with pre-fill, passive liveness, clear retry paths, and fallback document options	Configurable verification flow sequencing

Additional Commercial Considerations

PIX and Payment-Layer Risk

Brazil's PIX instant payment infrastructure creates a narrow fraud window. Operators need identity, device, and payment signals connected before withdrawal approval, not just at account registration. A bettor who passes KYC at registration but subsequently uses a mule PIX account creates AML exposure that document verification at onboarding alone cannot prevent.

Mobile-First Document Capture

The majority of Brazilian bettors are on board via mobile. Real-world document capture on mobile is subject to variables that laboratory-condition testing does not capture: low ambient light, older device cameras, laminated or physically damaged documents, and users unfamiliar with document photography requirements.

Peak-Volume Performance

Brazil's betting market surges during major football events. Operators should test their KYC infrastructure under projected peak load conditions. A document verification vendor that performs well at average volumes but degrades at peak load creates simultaneous compliance and conversion risks.

CPF Leakage and Multi-Accounting

The availability of leaked CPF data in Brazilian underground markets enables bonus abuse via multiple accounts, account farming for money laundering, and contas laranja operated by fraud networks. Biometric liveness detection is the most effective single control against these patterns because it requires a physical human face match, not just document and CPF data, before account activation.

Operators who want to see how Shufti manages the compliance-conversion balance across document verification, liveness, AML, and SIGAP in a single Brazil KYC flow can walk through the configuration with the team.

The KYC Vendor Test for Brazil Bets Operators

Selecting a KYC vendor for a .bet.br operator is a high-stakes compliance decision. A vendor failure cascades across every downstream obligation. The seven capabilities marked REQUIRED are non-negotiable. A vendor that is Partial or Not Met on any Required capability should not be selected.

Capability	What to Verify	Status	Priority	Evidence Required
Certified Biometric Liveness	Liveness detection certified against recognised PAD standards, such as ISO/IEC 30107-3 or iBeta PAD Level 1/2, from a SPA-recognised testing body. Confirm certification is current and covers the algorithm version in live production.	Met / Partial / Not Met	REQUIRED	Certificate + algorithm version
Multi-Format Document Verification	Handles all 27 Brazilian RG state formats without manual configuration. Also supports CNH, CIN, and a passport.	Met / Partial / Not Met	REQUIRED	Coverage list + tested state list
Real-Time CPF Validation	Real-time Receita Federal database query; exact name matching; active/ suspended/cancelled status detection.	Met / Partial / Not Met	REQUIRED	API integration documentation
SIGAP Integration	Native SIGAP API integration or documented integration pathway; automated blocking logic; balance return workflow; query scheduling.	Met / Partial / Not Met	REQUIRED	Integration spec + sandbox test results

LGPD Consent Management	Standalone biometric consent flow separate from ToS; timestamp capture; purpose-specific language; withdrawal mechanism; minimum 36-month retention per LGPD requirements.	Met / Partial / Not Met	REQUIRED	Consent flow spec + sample record
AML Screening: PEP + Sanctions	PEP lists: Brazilian domestic + international FATF-standard. Sanctions: 1,000+ sources minimum. Continuous screening with daily or more frequent refresh.	Met / Partial / Not Met	REQUIRED	Source list + refresh frequency
Audit Trail Exports	XML, XLS, and CSV export capability; granular event logging; minimum 36-month retention with redundant backup per Portaria 722 Article 25; SIGAP-compatible daily submission.	Met / Partial / Not Met	REQUIRED	Sample export + retention policy
Re-Authentication / MFA	Configurable 7-day and 30-minute inactivity triggers; SMS/email OTP, TOTP, biometric step-up; automated enforcement.	Met / Partial / Not Met	IMPORTANT	Re-auth configuration documentation
Age Assurance	Document DOB extraction + CPF age cross-reference + biometric face match; audit log of age verification decision.	Met / Partial / Not Met	IMPORTANT	Age assurance spec + decision log
Brazil-Compatible Data Handling	Whether the vendor can support Brazil-based processing/storage or documented cross-border transfer safeguards under LGPD.	Met / Partial / Not Met	IMPORTANT	Data handling and transfer documentation

Peak-Volume SLA	Uptime SLA at peak load (target 99.5%+); documented performance under surge conditions.	Met / Partial / Not Met	IMPORTANT	SLA document + load test results
Passive Liveness Option	Passive liveness detection available (no visible user action required).	Met / Partial / Not Met	OPTIONAL	Capability confirmation

RFP Question Bank

The following questions can be sent directly to prospective KYC vendors as part of a formal RFP or vendor evaluation conversation.

1. Can your platform verify CPF, RG (all 27 state formats), CNH, CIN, face match, certified liveness, AML screening, LGPD consent, and structured audit exports in one integrated workflow?
2. What is your current PAD certification level and from which SPA-recognised testing body? Which specific algorithm version is certified, and when was the certification last renewed?
3. Do you provide native SIGAP API integration or a documented integration pathway? What is your typical SIGAP query response time?
4. What is your document verification pass rate for Brazilian RG documents specifically? How do you handle RG state format variations?
5. How frequently do you refresh PEP and sanctions lists? What is your source count, and do you include Brazilian domestic PEP definitions?
6. How do you handle LGPD biometric consent: is it a standalone flow, and do you provide timestamped audit records with IP address capture?
7. What is your uptime SLA at peak load? Do you have load test data comparable to the major Brazilian sporting event traffic?
8. What audit trail export formats do you support, and can you provide a sample export showing the granularity of event logging?
9. Can you provide a sample Brazil betting audit export showing CPF result, document result, liveness result, AML result, SIGAP result, consent record, and final decision in one user timeline?
10. What fallback path do you provide when RG verification fails due to image quality, photograph aging, or unsupported format?

Can your platform separate compliance failures from image-quality failures in reporting, so operations teams can reduce false rejection without weakening controls?

Shufti combines all seven Required capabilities in one connected flow, CPF validation, multi-format document verification, iBeta PAD-certified liveness, SIGAP integration, continuous AML/PEP screening, LGPD consent management, and structured audit trail exports, purpose-built for licensed .bet.br operators.
Operators who want to see the Brazil KYC stack configured for their specific workflow can request a Brazil KYC demo or build and price a deployment directly.

How Exposed Is Your Current KYC Stack?

Score your current KYC stack by awarding 1 point for each control that is fully implemented. Be honest: partially implemented controls score 0 until they are complete and tested in production.

Control	Score	Notes
CPF validation with real-time Receita Federal check	☐	
Document verification covering all 27 RG state formats	☐	
Biometric liveness certified against recognised PAD standards	☐	
Age assurance beyond checkbox: document DOB + face match	☐	
SIGAP integration with automated blocking within 72 hours	☐	
Continuous AML/PEP screening with daily list refresh	☐	
Standalone LGPD biometric consent with audit retention	☐	
7-day re-verification enforced automatically	☐	
Structured audit trail exportable in XML, XLS, CSV	☐	

Scoring Guide

0-4: High exposure. Multiple compliance gaps require urgent remediation.

5-7: Partial readiness. Key gaps remain. Prioritise SIGAP automation and audit trail completeness.

8-9: Strong readiness. Review evidence requirements before an inspection request arrives.

Operators who scored below 8 and want to see Shufti's connected Brazil KYC flow configured for their workflow can request a product walkthrough.

30/60/90-Day Implementation Roadmap

A typical licensed .bet.br operator requires 90 days to achieve full Portaria 722/1,143 compliance from project start. The roadmap below sequences implementation to address the highest-risk gaps first.

Days 1-30: Assessment and Vendor Selection

- Audit current KYC flow against all SPA/MF ordinances using the Regulatory Control Map
- Document capability gaps: document verification pass rate, liveness certification status, SIGAP integration readiness
- Issue vendor RFP using the RFP Question Bank; score responses against Vendor Evaluation Scorecard
- Begin internal audit trail design: identify what events must be logged and in what format
- Assess SIGAP integration readiness
- Engage legal team to review LGPD biometric consent form and Lei 15.211/2025 age assurance obligations

Days 31-60: Implementation and Integration

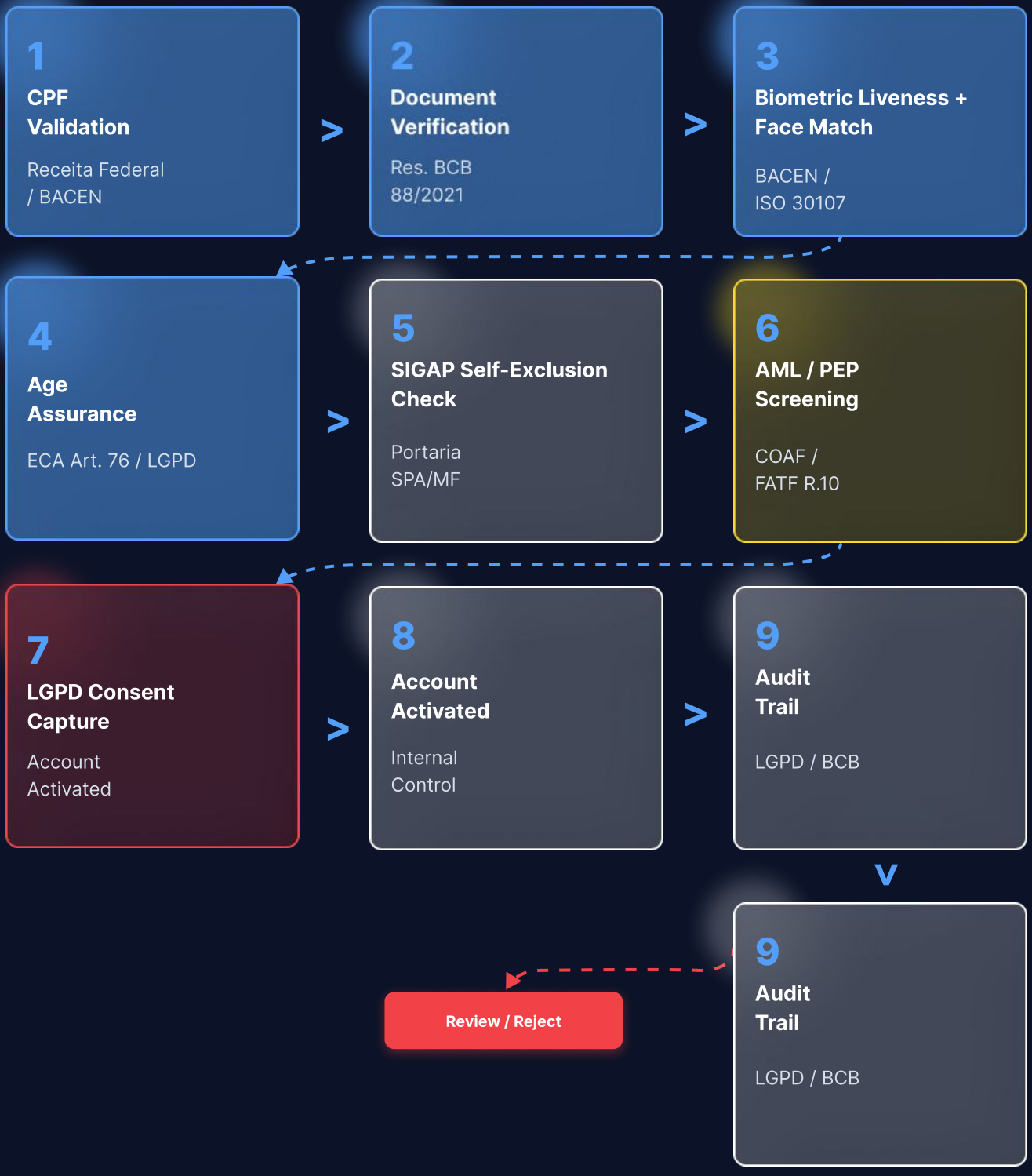
- Finalise vendor selection; execute contract; begin technical integration
- Implement multi-format document verification; run pass-rate benchmarks before going live
- Configure 7-day re-verification and 30-minute inactivity triggers; test with simulated user sessions
- Build a standalone LGPD biometric consent flow; integrate into the onboarding journey; test consent record logging
- Develop SIGAP integration; test automated blocking logic in sandbox environment
- Build audit trail export automation; provision redundant backup storage meeting 36-month minimum retention per Portaria 722 Article 25
- Implement continuous PEP and sanctions screening with a daily list refresh; configure SISCOAF export format
- Configure risk-based transaction monitoring per Portaria 1,143 and implement SISCOAF reporting workflow for suspicious transactions
- Review age assurance implementation against Lei 15.211/2025 requirements

Days 61-90: Testing, Audit, and Certification

- Conduct an internal compliance audit: sample 20 users and verify all KYC steps are logged correctly in the audit trail
- Review audit trail exports in XML, XLS, and CSV formats; verify completeness, event granularity, and correct timestamp formatting (ISO 8601)
- Load-test new verification flows at projected peak traffic volumes (target 99.5%+ uptime under peak load)
- Measure onboarding conversion impact: compare registration completion rate and time-to-first-deposit before and after implementation
- Conduct SIGAP integration end-to-end testing: simulate self-exclusion notification and verify automated blocking within a 24-hour internal target
- Conduct disaster recovery drill: backup restoration and data integrity verification against the 36-month minimum retention requirement per Portaria 722 Article 25
- Validate PEP screening accuracy with test accounts; confirm SISCOAF export format is accepted by COAF
- Confirm liveness certification is current and covers the algorithm version in production
- Document implementation for regulatory evidence: retain vendor contracts, certification documents, integration specifications, and test results

KYC COMPLIANCE WORKFLOW — BRAZIL

BACEN · COAF / FATF · LGPD · SIGAP · Receita Federal



How Shufti Supports Brazilian Betting Operators

Brazil .bet.br operators do not need more isolated checks. They need a connected identity workflow that can prove who the bettor is, whether they are eligible to play, whether they create AML or fraud risk, and whether every decision can be reconstructed for audit.

Brazil Requirement	Operator Challenge	Shufti Capability	Performance
CPF Validation (Portaria 722/1,143)	CPF alone does not stop mule accounts or synthetic identity fraud: it is an eligibility gate, not an identity control	CPF + document verification + biometric face match in a single connected workflow; real-time Receita Federal integration with exact name-matching	Real-time API response
Biometric Liveness (Portaria 722)	Non-certified liveness is a direct Portaria 722 violation; static selfies create spoofing risk	iBeta PAD Level 1 and Level 2 certified active and passive liveness; proprietary deepfake and presentation attack detection; silicone mask and face-swap attack coverage	98.22% acceptance rate; 2.98s response time*
Document Verification (Portaria 722/1,231)	27 RG state format variations create elevated friction; narrow-trained vendors produce 50%+ false rejection for RG	Multi-format document verification across 10,000+ document types from 245+ countries; all 27 Brazilian RG state formats supported without manual configuration	90.25% acceptance rate; 0.15% false positive rate*
AML / PEP Screening (Portaria 1,143)	PEP status changes over time; registration-only screening is non-compliant; SISCOAF reporting requires structured output	Continuous AML screening with PEP list refresh; domestic and international PEP coverage; SISCOAF-compatible reporting	1,700+ sources; 20M+ records; continuous monitoring with real-time alerts*

SIGAP / Self-Exclusion (Regulatory Instruction No. 31)	Manual blocking creates 72-hour breach risk and audit exposure; liability applies from notification receipt, not review decision	SIGAP integration support with automated blocking workflows and timestamped audit logs for notification receipt, blocking action, and balance return	Integration support is subject to the operator platform architecture
LGPD Biometric Consent (Lei 13.709/2018)	Consent must be standalone, purpose-specific, timestamped, and retained for 5 years: bundled ToS consent is non-compliant	LGPD-compliant standalone consent capture; timestamp and IP address logging; audit-ready consent records integrated into verification flow	Integrated into the verification workflow
Audit Trail (Portaria 722)	Regulators require structured, exportable evidence with granular event logging: screenshots and platform logs are insufficient	Structured audit trail exports in XML, XLS, and CSV; granular event logging with ISO 8601 timestamps; minimum 36-month retention supported	Export-ready on demand
Re-Authentication (Portaria 722)	7-day and 30-minute inactivity triggers must be automated and enforced consistently: manual enforcement creates audit gaps	Behavioural biometrics for passive continuous authentication; adaptive MFA step-up with configurable triggers; SMS, email OTP, TOTP, and biometric step-up	Configurable trigger management

*Performance metrics are based on Shufti platform data across global verification volumes as of Q1 2026. Individual operator performance varies based on document quality, user behaviour, mobile capture conditions, and configuration. Brazil-specific benchmarking should be completed during implementation because RG/CNH/CIN distribution, mobile capture quality, and user demographics materially affect pass rates.

Operators with a specific Brazil KYC architecture in mind can build and price a deployment plan directly without going through a sales process.

98.22%

biometric liveness acceptance rate

2.98s

average liveness verification response time

Appendix A: Internal Audit Checklist

Use this checklist in a pre-enforcement internal compliance review. Complete each row with verified status and supporting evidence before submitting to internal compliance committees or in response to SPA audit requests.

Control	Verified
CPF validation: real-time Receita Federal integration confirmed and tested	☐ Yes ☐ No
Document verification: tested across all 27 RG state formats; pass rate benchmarked	☐ Yes ☐ No
Liveness detection: certification verified; algorithm version in production confirmed	☐ Yes ☐ No
7-day re-verification: automated logic tested; audit trail logging confirmed	☐ Yes ☐ No
30-minute inactivity re-auth: automated trigger tested	☐ Yes ☐ No
SIGAP integration: automated blocking tested; balance return workflow confirmed	☐ Yes ☐ No
PEP screening: continuous screening confirmed; list refresh frequency verified	☐ Yes ☐ No
LGPD biometric consent: standalone consent flow implemented	☐ Yes ☐ No
Age assurance: document DOB + face match implemented	☐ Yes ☐ No
Audit trail exports: XML, XLS, CSV exports generated and verified	☐ Yes ☐ No
Disaster recovery: backup restoration tested; data integrity verified	☐ Yes ☐ No
Certification currency: confirmed certificate covers algorithm version in production	☐ Yes ☐ No

Regulatory Contacts

1. SPA (Secretaria de Premios e Apostas): Pre-audit consultations and regulatory clarification. gov.br/fazenda/pt-br/acesso-a-informacao/institucional/secretarias/secretaria-de-premios-e-apostas
2. ANPD (National Data Protection Authority): LGPD compliance clarification and DPIA guidance. gov.br/anpd/pt-br
3. COAF (Financial Intelligence Unit): SISCOAF reporting guidance and AML obligations. gov.br/fazenda/pt-br/orgaos/coaf

Recommended External Review

1. Legal review of LGPD biometric consent documentation against current ANPD guidance
2. Third-party compliance audit of full KYC implementation against the Portaria 722 checklist
4. Penetration testing of the liveness detection system against known deepfake samples
5. Brazilian legal counsel review of Lei 15.211/2025 age assurance obligations

Shufti

Verify .bet.br Players With a Connected KYC Stack

Shufti's Brazil KYC stack combines CPF validation, multi-format document verification, iBeta PAD-certified liveness detection, SIGAP integration, continuous AML/PEP screening, LGPD consent management, and structured audit trail exports in one integrated flow, purpose-built for licensed .bet.br operators.

Request a Brazil KYC Demo

shuftipro.com
sales@shuftipro.com