Shufti

Singapore

GUIDE

KYC Readiness Guide for Singapore

MAS AML/CFT Controls, NRIC Authentication Migration, MyInfo and FIN-Holder Onboarding Workflows, Source-of-Wealth Evidence Standards, and AI Fraud Defence

VÉRIFICATION D'ÂGE KJM

PCI DSS

iBeta Niveau 1

ISO 27001: 2013

CE+

QG GDPR

SOC2

GDPR

CCPA

Executive Summary

Singapore's regulatory and fraud environment for financial institutions shifted fundamentally after 2023. The S$3 billion money laundering case exposed specific, repeatable control failures across nine of the country's most reputable institutions. MAS responded with S$27.45 million in enforcement penalties in July 2025, a National AML Strategy, the COSMIC inter-bank information sharing platform, and tightened expectations across customer risk assessment, source-of-wealth corroboration, transaction monitoring, and enhanced due diligence.

The challenge is that the obligations are not new. They are being executed more consistently and with more evidence, or they are not. At the same time, two parallel pressures are making the compliance task harder.

NRIC numbers can no longer serve as authentication credentials after 31 December 2026. Institutions must rebuild core authentication workflows before enforcement begins. And fraud sophistication, including deepfake video attacks, synthetic identity fraud, and organised mule recruitment, is exposing gaps in onboarding controls that were designed for a lower-capability threat environment.
This guide gives compliance, fraud, and operations teams the frameworks to address all three. It provides a regulatory map by institution type, a breach-to-control remediation matrix drawn from MAS enforcement findings, and a six-segment customer verification model that correctly accounts for Singapore citizens, FIN holders, new arrivals, non-residents, foreign corporate UBOs, and PSP/DPT users.

It also contains a phased NRIC authentication migration checklist, a source-of-wealth evidence matrix with nine wealth-source categories, and an IDV vendor evaluation scorecard with sixteen criteria calibrated to Singapore-specific regulatory requirements.

It is written for Chief Compliance Officers, MLROs, Heads of Fraud, and Product Operations leaders at Singapore-licensed banks, payment service providers, fintechs, and wealth managers.

The institutions that navigate this period most effectively will be those that treat KYC, AML, and fraud prevention as connected execution disciplines, not separate compliance checkboxes managed in isolation.

The institutions that navigate this period most effectively will be those that treat KYC, AML, and fraud prevention as connected execution disciplines, not separate compliance checkboxes managed in isolation.

Table of Contents

Why Singapore's KYC Environment Changed After 2023

On 15 August 2023, the Singapore Police Force arrested ten foreign nationals in connection with a S$3 billion money laundering network. The investigation uncovered proceeds linked to overseas fraud, illegal gambling, and other serious crimes, routed through Singapore financial institutions using falsified documentation, opaque corporate structures, and unverified source-of-wealth claims. It was the largest money laundering case in Singapore's history.

The scandal did not change Singapore's status as a leading financial centre. It changed the enforcement expectations placed on institutions operating within it.

MAS's subsequent review identified five failure patterns:

1. Inadequate customer risk assessment at onboarding
2. Failure to establish and independently corroborate the source of wealth for high-value customers
3. Insufficient review of transaction monitoring alerts
4. Weak enhanced due diligence procedures that existed on paper but were inconsistently applied
5. Governance structures that allowed compliance frameworks to lag behind business growth

The Regulatory Response

The National AML Strategy, published on 30 October 2024 by MAS and the Ministry of Finance, set out a three-pronged approach: proactive prevention through stronger pre-onboarding controls; active detection using analytics, transaction monitoring, and inter-agency information sharing; and firm enforcement with proportionate penalties for failures at any institutional scale.

COSMIC: Industry-Wide Information Sharing

On 1 April 2024, MAS launched COSMIC (Collaborative Sharing of ML/TF Information and Cases), a centralised platform enabling financial institutions to share customer information in cases involving potential money laundering, terrorism financing, or proliferation financing. Initial participants: DBS, HSBC, OCBC, Standard Chartered, UOB, and Citibank (Singapore).

COSMIC increases the sector's ability to identify cross-institution suspicious patterns, particularly where a customer presents risk signals across participating banks.

MAS operates the platform as the centralised hub: financial institutions submit flagged customer information to MAS, which makes it available to other participating institutions. This is cross-institutional data sharing facilitated by MAS, not direct MAS surveillance of customer activity.

The practical consequence for institutions with weak controls is significant, as suspicious activity that might be invisible to one institution acting alone may become visible when customer information is shared across the network.

The July 2025 Enforcement Action

MAS announced enforcement actions against nine financial institutions on 4 July 2025.

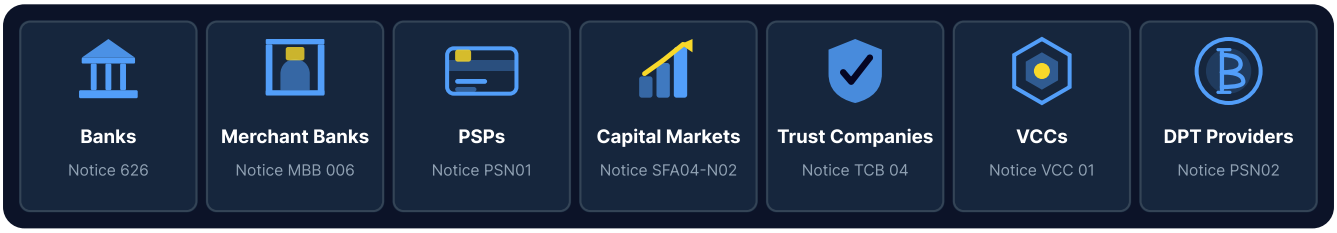
The institutions and penalties: Credit Suisse (Singapore) S$5.8 million, UOB S$5.6 million, Citibank Singapore S$2.6 million, UBS Singapore S$3 million, UOB Kay Hian S$2.85 million, Julius Baer S$2.4 million, Blue Ocean Invest S$2.4 million, LGT Bank S$1 million, Trident Trust S$1.8 million. Total: S$27.45 million.

Scale and reputation did not determine exposure. The quality of control execution did.

August 2023	1 April 2024	30 Oct 2024	July 2025
S$3B scandal	COSMIC	National AML Strategy	S$27.45M enforcement

Singapore's Regulatory Architecture by Institution Type

MAS Notice 626 governs banks and receives the most coverage in compliance literature, but it applies specifically to banks. Singapore's broader financial sector operates under a network of separate AML/CFT notices and frameworks. Compliance teams at non-bank institutions frequently under-scope their obligations by treating Notice 626 as the universal reference.



Notice Map: Which Framework Applies to Your Institution

Institution Type	Primary AML/CFT Notice	Licensing Framework	Obligations	Why It Matters for IDV Workflow Design
Banks	MAS Notice 626	Banking Act	CDD, SoW, EDD, transaction monitoring, STR filing	Higher scrutiny on SoW, EDD application, alert review, and audit evidence; on-premise deployment may be required for data residency

Merchant Banks	MAS Notice 1014	Banking Act	Equivalent obligations to Notice 626	Same verification depth as banks; smaller volumes may allow more manual EDD workflows
Payment Service Providers	MAS Notice PSN01	Payment Services Act 2019	CDD, AML screening, transaction monitoring; obligations scale with licence class	High-volume, low-value onboarding; tolerance for manual review delays is lower; automated routing is essential
Capital Markets Intermediaries	SFA AML/CFT Notices	Securities and Futures Act	CDD, EDD for PEPs, SoW for high-risk clients	Client base often includes PEPs and high-net-worth non-residents; SoW workflow and EDD depth are the design priorities
Trust Companies	TCA-N03	Trust Companies Act	Enhanced beneficial ownership obligations	Deep UBO tracing and legal arrangement verification; complex corporate structures require KYB at depth
Variable Capital Companies	VCC-N01	VCC Act	Fund-level and sub-fund AML/CFT requirements	Beneficial ownership tracing through fund structures; sub-fund verification may be needed separately
DPT Service Providers	Payment Services Act 2019 framework and applicable MAS notices for digital payment token services	Payment Services Act 2019	CDD, sanctions screening, Travel Rule-related controls, transaction monitoring	Wallet screening, Travel Rule for crypto asset transfers, on-chain transaction monitoring; blockchain-native risk signals required

Obligations Beyond Notice 626

The Payment Services Act 2019 is the primary framework for payment service providers and DPT providers, requiring customer identification, AML screening, transaction monitoring, and suspicious transaction reporting obligations calibrated to licence class.

Compliance teams at non-bank entities that have structured their controls primarily around Notice 626 should review their specific applicable notice and confirm that their verification platform supports the distinct obligations, including PSN01 thresholds for payment transactions, DPT Travel Rule workflows, and TCA-N03 beneficial ownership depth requirements.

The Enforcement Reality: What MAS Is Actively Penalising

What the July 2025 Penalties Reveal

The July 2025 enforcement action provided a level of specificity about MAS's enforcement expectations that supervisory circulars rarely achieve. Four distinct failure categories appear across the published penalty summaries. Each corresponds to a specific control gap, and each maps directly to remediation actions that institutions must implement before the next supervisory cycle.

Policy Existence Is Not the Standard

Every penalised institution had written compliance policies. The failures were in execution: procedures were inconsistently applied, evidence was insufficiently generated, and governance structures tolerated the gap between what policies said and what staff actually did.

Breach Category	What MAS Found	Evidence MAS Would Expect	Required Control Response
Customer Risk Assessment	Institutions accepted high-value customers without adequate risk profiling; risk ratings were not updated as profiles changed	Documented risk rationale per customer; approval records for tier upgrades; review trail for higher-risk categories	Risk engine with configurable scoring; documented escalation for rating changes
Source of Wealth Corroboration	SoW documentation collected but not independently verified; beneficial owners not identified; conflicting information not resolved	Independent corroboration documents; discrepancy notes with resolution; beneficial ownership chain with verified identities	SoW workflow with evidence checklist; MLRO review gate for unresolved discrepancies
Transaction Monitoring and Alert Review	Monitoring systems flagged suspicious transactions; institutions did not adequately review or escalate alerts	Case notes for each reviewed alert, escalation records, SLA compliance evidence, and SAR filing decisions with rationale	Case management system with SLA enforcement; audit trail on every reviewed alert
Enhanced Due Diligence	EDD procedures in policy documents; not consistently applied for higher-risk customers; escalation paths not followed	EDD checklist completion per higher-risk customer; approval from compliance committee or MLRO; periodic review schedule	Tiered onboarding workflow with mandatory EDD gates for higher-risk segments

Compliance teams can use these questions as an internal diagnostic. Before the next supervisory cycle, four questions are worth asking:

- Can your institution prove why a specific customer was assigned their current risk tier, including who made that decision and when?
- Can your institution show who reviewed the source-of-wealth evidence for each higher-risk customer, and what they concluded?
- For every alert closed in the past 12 months, can your institution produce the case note, the reviewer's name, and the rationale?
- For each higher-risk customer, can your institution show when EDD was triggered, who approved it, and what the periodic review schedule is?

These are the questions MAS supervisors ask. Institutions that cannot answer them consistently are exposed.

Singapore Customer Segments and Verification Pathways

The framing of 'citizens and permanent residents onboard instantly, non-citizens face manual delays' is commercially useful but operationally incomplete.

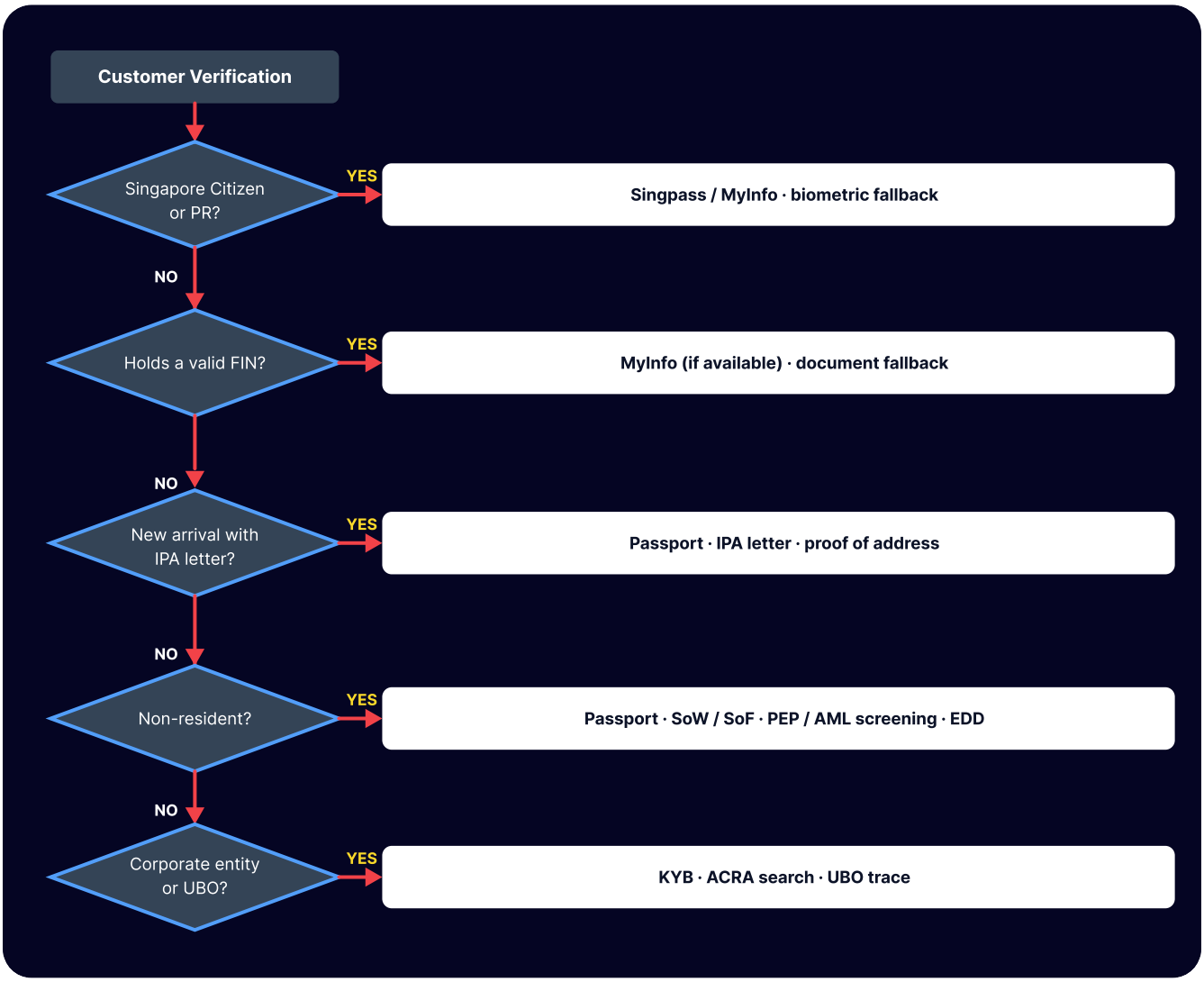
The central corrective: FIN (Foreign Identification Number) holders with valid Employment Passes, S Passes, Dependant Passes, and Long-Term Visit Passes are eligible for Singpass registration and may have MyInfo profiles, provided they are aged 15 or above and hold a valid pass issued by ICA.

MyInfo data completeness for FIN holders varies. A customer who arrived recently may have limited government-held data populated. The practical verification design must account for data gaps through document-based fallback flows.

Customer Segment	Typical Verification Path	MyInfo Eligible?	Friction	Controls Required
Singapore Citizens and PRs	Singpass/MyInfo with consent	Yes, full data	Low	MyInfo integration + biometric fallback
FIN-Holding EP/ S Pass Holders	Singpass/MyInfo, where available; document fallback for data gaps	Potentially, if eligible for Singpass and the data profile is available	Low-Medium	MyInfo + pass validity + address verification
New Arrivals with IPA Letters	Document verification + pass validation	Limited: Singpass may not yet be active	Medium	Passport, IPA letter, employment confirmation, and address workflow
Non-Resident Investors and Directors	Passport + address + SoW/SoF + PEP/ sanctions screening	No	High	Global document coverage + EDD workflow

Foreign Corporate UBOs	KYB: registry checks + UBO verification + beneficial ownership trace	No	Very High	ACRA for Singapore entities; global KYB for foreign principals
DPT/PSP Wallet Users	Document + biometric + transaction monitoring	Depends on residency status	Varia ble	Low-friction IDV + fraud signals + Travel Rule for DPT

Note: Singpass eligibility does not guarantee complete MyInfo data. FIN holders who registered recently may have partial profiles. Platforms must support document-based fallback flows for data gaps.



Practical Workflow Design

An institution onboarding a customer without first establishing which segment that customer belongs to will apply either under-verification (treating a high-risk non-resident as equivalent to a Singapore citizen) or over-verification (requiring document uploads from a FIN holder with a complete MyInfo profile). Both outcomes carry costs: the first is a compliance failure; the second is onboarding abandonment.

The practical design question: does the institution's verification platform support conditional routing, directing the customer to the appropriate path based on declared or detected identity signals at the start of the flow? Platforms with fixed single-path onboarding cannot accommodate Singapore's segmentation requirements without manual intervention.

The Fraud Threat at Onboarding

Singapore's identity fraud environment has shifted materially over the past two years. Three fraud typologies are now driving onboarding-stage losses: deepfake video fraud, synthetic identity attacks, and organised mule account recruitment.

Deepfake Video Fraud

Deepfake fraud uses AI-generated synthetic video, created from publicly available photographs or social media footage of a real person, submitted during liveness checks to impersonate that individual. The attack bypasses liveness detection systems that check for movement, blinking, and face tracking but do not analyse the pixel-level signatures of AI-generated content.

The Singapore Police Force and Cyber Security Agency have both highlighted AI-generated fraud as an escalating concern in their respective 2024 advisory publications. iBeta PAD Level 1 and Level 2 certification on a liveness solution confirms it can defeat spoofing attacks using static images, pre-recorded video, and 3D masks. It does not, by itself confirm capability against modern injection attacks or AI-generated video. Institutions should request specific test evidence from vendors on deepfake, replay, screen presentation, and digital injection attack types, not iBeta certification alone.

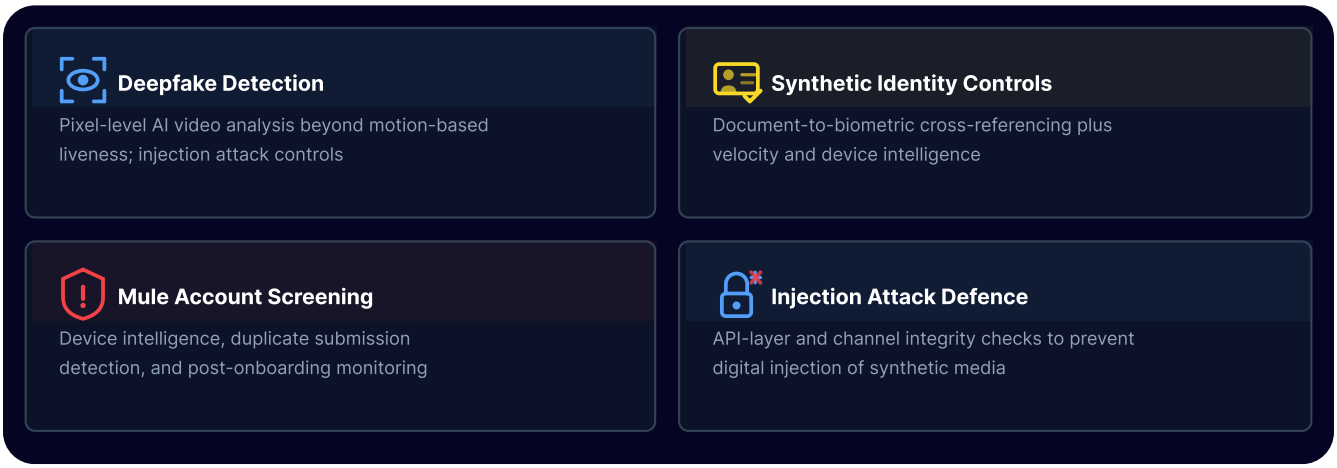
Synthetic Identity Fraud

Synthetic identity fraud combines fabricated identity information (name, date of birth, address, document numbers) with real or stolen biometric data. The resulting identity does not correspond to a real person, which means traditional database checks find no match. Detection requires cross-referencing document metadata against biometric data, identifying mismatches between stated biographical information and the biometric characteristics presented, combined with velocity and device intelligence signals.

Mule Account Onboarding

The Singapore Police Force placed 550 individuals under banking restrictions and 801 under telecommunications restrictions for mule-related activity as of February 2026. Mule accounts differ from synthetic identity fraud in that both the identity document and the biometric data are genuine. The recruited individual passes standard KYC controls. The risk signal is behavioural: the account's first-transaction-to-onboarding interval, transaction pattern velocity, and the relationship between stated occupation and actual account activity.

Fraud Type	Why Standard KYC Fails	Required Control	Design Implication
Deepfake Video	Liveness checks detect movement but not AI-generated pixel patterns	Anti-deepfake detection with injection attack controls	Ask vendors for evidence beyond iBeta PAD; request deepfake-specific test data
Synthetic Identity	Identity document may be fabricated; biometric data is real; no existing fraud list match	Document-to-biometric cross-referencing plus velocity and device intelligence signals	Detection requires metadata analysis, not just format validation
Mule Account	Real person, real document, real biometric; standard KYC cannot detect recruited accounts	Behavioural signals, device intelligence, and post-onboarding transaction monitoring	First-transaction-to-onboarding interval and account velocity are the primary signals
Digital Injection Attack	Fraudster bypasses the camera entirely by injecting synthetic media at the API layer	API and channel integrity checks to prevent injection	Passive liveness is not sufficient; channel-level controls are required



Compliance teams that want to validate that their current liveness and biometric controls can withstand Singapore's 2026 fraud threat model, including deepfake video, injection attacks, and synthetic identity patterns, can request a walkthrough showing how Shufti handles deepfake video, injection attacks, and synthetic identity detection, *calibrated to APAC fraud patterns*.

The NRIC Authentication Migration

31 December 2026

PDPC enforcement begins 1 January 2027

On 2 June 2025, MDDI, the Personal Data Protection Commission (PDPC), and the Cyber Security Agency of Singapore (CSA) issued a joint advisory establishing that private organisations must stop using NRIC numbers as authentication credentials by 31 December 2026.

Identification vs. Authentication: A Critical Distinction

PERMITTED (identification):

Collecting NRIC during KYC onboarding for AML/CFT compliance
Using NRIC as an internal unique customer identifier
Requesting NRIC to identify a customer during service interaction

PROHIBITED from 31 December 2026 (authentication):

Using NRIC as passwords or PINs
Setting NRIC as a default or reset credential
Combining NRIC with easily obtainable personal data (DOB, address) to form authentication factor
Using NRIC as a security credential that controls access to account or service

Note: The legal and operational distinction: Identification means collecting an NRIC number to establish who a customer is. This remains required under MAS Notice 626. Authentication means using the NRIC number to verify that the person claiming an identity is who they say they are: passwords, PINs, and access codes. The December 2026 ban applies to authentication only. Institutions must maintain NRIC collection for CDD compliance while eliminating it from every authentication flow.

NRIC Authentication Migration Checklist

Discovery Phase

- ☐ Map all customer-facing authentication flows that currently accept NRIC
- ☐ Identify backend systems using NRIC as a default password
- ☐ Document call-centre authentication procedures using NRIC
- ☐ Identify password reset flows that rely on NRIC

Architecture Phase

- ☐ Select replacement authentication methods (biometric, MFA, device-bound credentials)
- ☐ Design fallback flows for customers unable to complete biometric authentication
- ☐ Assess if Singpass-based authentication via MyInfo is appropriate

Implementation Phase

- ☐ Notify customers of authentication changes with sufficient lead time
- ☐ Update call-centre authentication scripts and train agents
- ☐ Run parallel systems through transition period
- ☐ Conduct fraud risk assessment for migration period

Institutions with complex legacy systems should note that the implementation window is now under eight months from April 2026. Large institutions that have not commenced vendor procurement face a significant risk of non-compliance.

Institutions that have mapped their NRIC authentication dependencies and want to see how biometric replacement, Singpass integration, and MFA can cover each use case before the 31 December 2026 deadline can walk through the platform configuration with the Shufti team, covering biometric replacement, Singpass integration, and MFA.

Source of Wealth Evidence Standards

Source of Wealth (SoW) verification has become a defining test of compliance quality in Singapore following the July 2025 enforcement action. Multiple penalised institutions collected SoW documentation but failed to establish that stated wealth origins were independently corroborated, sufficiently specific to the customer's claimed wealth level, or consistent with the customer's profile and conduct.

The distinction between collecting documentation and actually verifying wealth origins is the enforcement gap MAS exploited. Institutions that treat SoW as a documentation exercise rather than an evidence-assessment exercise remain exposed.

SoW versus Source of Funds: Operational Distinction

Source of Funds (SoF):

Verification of funds for a specific transaction. Required for wire transfers from non-established customers and for high-risk transactions regardless of amount.

Source of Wealth (SoW):

The total accumulated wealth of the customer. Required for PEPs, customers from high-risk jurisdictions, customers with high-value or complex beneficial ownership structures. SoW is an ongoing obligation and must be refreshed when circumstances materially change.

The MAS 2025 amendment to Notice 626 strengthened corroboration expectations: institutions are expected to obtain independent documentation sufficient to confirm the stated wealth source, document how they assessed the sufficiency of that evidence, and record what action they took when evidence was insufficient or conflicting.

SoW Evidence Sufficiency Matrix (Continued)

Wealth Source	Acceptable Primary Evidence	Independent Corroboration Required	Red Flags
Employment Income	3-6 months payslips; employment contract; bank statements showing salary deposits	Employer confirmation letter, tax assessment; company verification via registry	Salary level inconsistent with employer size; unexplained large deposits
Business Ownership and Proceeds	Company financial statements, business registration documents, and tax returns	Independent auditor's report; company registry verification (e.g. ACRA); corporate tax assessment	Offshore structures without a clear business purpose; undocumented related-party transactions
Investment Returns	Brokerage statements; portfolio valuations; custodian confirmations	Independent custodian or manager confirmation; stock exchange verification for listed holdings	Returns disproportionate to stated investment experience; unexplained offshore accounts
Inheritance	Will or probate documents; executor's confirmation; estate valuation	Solicitor's certificate or court probate record	Contested or informal inheritance claims; missing probate documentation
Property Sales	Sale and purchase agreement; title transfer records; settlement statement	Land registry confirmation; solicitor's completion letter	Property in a high-risk jurisdiction; sale price inconsistent with market data
Gifts	Signed gift declaration; evidence of donor's wealth; relationship explanation	Donor's wealth documentation; legal declaration where appropriate	Large gifts from undocumented sources; gift structure resembling transaction disguise
Digital Asset and Crypto Wealth	Blockchain wallet statements, exchange account statements, transaction history	Exchange-level KYC confirmation; on-chain analysis report	Wallet activity linked to mixing, high-risk exchanges, or dark web indicators

Offshore Corporate Proceeds	Company sale or dividend documentation; shareholder register; company accounts	Independent company valuation or auditor's report; offshore registry confirmation	Offshore structures with opaque ownership or jurisdictions without public registries
Trust or Family Office Distributions	Trust deed; trustee confirmation; distribution statement	Independent trustee confirmation; trust registration documentation	Discretionary trusts with undisclosed settlors; distributions inconsistent with stated trust purpose

Handling Discrepancies

When collected evidence is inconsistent with the customer's stated profile, incomplete, or raises credibility concerns, institutions should document the discrepancy, the questions asked to resolve it, and the resolution reached. If the discrepancy cannot be resolved, the case should be escalated to the MLRO with a recommendation on continuing or exiting the relationship. MAS does not expect institutions to achieve certainty. It expects institutions to demonstrate that they applied professional scepticism and documented their reasoning.

Singapore KYC Operating Model

A compliant Singapore KYC operating model is not a single set of procedures. It is a tiered, segment-responsive system that applies the right depth of verification to each customer type while generating the audit evidence that MAS expects to find in a supervisory review.

Structure of a Compliant Operating Model

Step	System Owner	Evidence Produced	Failure Risk
1. Customer Segment Identification	Product / Operations	Segment determination rationale, documented	Wrong verification path selected
2. Verification Pathway Selection	Product / Operations	Routing record on a segment basis	Over-verification or under-verification applied
3. Identity and Document Verification	Technology / Compliance	Verification result, document images, data extracted	Fraudulent document missed; OCR error accepted
4. Biometric and Fraud Screening	Technology / Fraud Ops	Liveness result, fraud signal log, deepfake assessment	AI-generated video not detected
5. AML and Sanctions Screening	Compliance	Screening result with timestamp, source lists checked	Sanctioned or PEP customer missed
6. Risk Tier Assignment	Compliance	Risk tier record with rationale and approver	High-risk customer rated as standard
7. Source of Wealth Verification	Compliance / MLRO	Evidence checklist, sufficiency assessment, discrepancy notes	SoW collected but not corroborated or assessed
8. Corporate and UBO Verification	Compliance / Legal	KYB report, UBO chain, registry confirmations	Beneficial owner not identified to the natural person level
9. Ongoing Monitoring	Fraud Ops / Risk	Alert log, case notes, review decisions with rationale	Alerts closed without a documented rationale
10. Audit Evidence Preservation	Compliance / Operations	Consolidated case record with all step outputs	Incomplete record; cannot reconstruct decision trail

Key Operating Model Steps

Step 1: Customer Segment Identification

Before initiating any verification procedure, determine which segment the customer belongs to: Singapore Citizen or PR, FIN-holding resident, new arrival, non-resident, foreign corporate UBO, or PSP/DPT user.

Step 2: Verification Pathway Selection

SC/PR and FIN holders with Singpass access are routed to MyInfo-based verification with biometric confirmation. New arrivals and non-residents are routed to document verification.

Step 4: Biometric Verification and Fraud Screening

Capture biometric confirmation. Run anti-deepfake and injection attack detection. Apply device intelligence and velocity screening.

Step 6: Risk Tier Assignment

Assign a documented risk tier (standard, enhanced, or EDD) based on nationality, industry, transaction profile, beneficial ownership complexity, and PEP status.

Step 7: Source of Wealth Verification

For PEPs, customers from high-risk jurisdictions, and customers with high-value wealth levels: initiate SoW collection using the evidence matrix. Document sufficiency assessment.

Step 7: Source of Wealth Verification

For PEPs, customers from high-risk jurisdictions, and customers with high-value wealth levels: initiate SoW collection using the evidence matrix. Document sufficiency assessment.

Step 8: Corporate and UBO Verification

For corporate customers, verify legal existence via ACRA (for Singapore entities) or equivalent overseas registry. Trace beneficial owners to the natural person level. Verify each UBO individually using the personal verification pathway appropriate to their segment.

Step 9: Ongoing Monitoring and Periodic Review

Post-onboarding monitoring should flag transactions inconsistent with the customer's stated wealth and business profile, sudden changes in transaction volume or counterparty geography, and account activity indicators associated with mule recruitment. Higher-risk customers require periodic review at defined intervals.

Step 10: Audit Evidence Preservation

Every step should generate a case record documenting: segment determination rationale, verification pathway selected, evidence collected and assessed, risk tier assigned, SoW/SoF outcome, AML screening results, EDD completion or escalation, and any suspicious transaction referral decision.

Selecting an IDV Platform: Evaluation Criteria for Singapore

Why Platform Selection Is a Near-Term Decision

Three regulatory and operational forces make IDV platform selection a near-term procurement decision for Singapore financial institutions. The NRIC authentication deadline is 31 December 2026. MAS enforcement has demonstrated that implementation gaps carry penalty risk, not policy gaps. And the fraud environment requires controls that were not standard in platforms designed for a 2020-era threat model.

The evaluation criteria below are calibrated to Singapore-specific requirements. They are written in the language of a compliance evaluator, not a technology buyer.

Evaluation Criterion	Regulatory Requirement	Evaluation Question	Must-Have?
Singpass/MyInfo Integration	MAS Notice 626 CDD; Singapore digital identity infrastructure	Does the platform offer native MyInfo integration with document fallback for FIN holders with incomplete profiles?	Yes
Document Coverage (10,000+ types, 240+ countries)	MAS's obligation to verify non-citizen identity	What is the documented coverage of Employment Pass categories, APAC passport variants, and IPA letters?	Yes
Anti-Deepfake and Injection Attack Detection	NRIC authentication replacement requires biometric integrity	What attack types has the vendor tested beyond the iBeta PAD scope? Request deepfake, replay, screen, and injection evidence.	Yes

AML Screening with Singapore-Specific Lists	MAS Notice 626 screening obligations	Does the platform screen against MAS domestic lists alongside OFAC, UN, EU, and adverse media? What is the update frequency?	Yes
Source-of-Wealth Workflow Support	July 2025 MAS enforcement findings	Does the platform support configurable SoW evidence collection with a documented case trail?	Yes
On-Premise Deployment Option	MAS TRM Guidelines: data residency requirements	Can the platform deploy on-premise or private cloud for institutions with data localisation requirements?	For banks and larger institutions
Configurable Risk-Tiered Routing	Risk-based CDD; Singapore six-segment customer model	Can the platform route customers to different verification depths based on nationality, segment, and risk score without manual intervention?	Yes
Beneficial Ownership and KYB	Corporate CDD; ACRA verification for Singapore entities	Does the platform integrate with ACRA and provide UBO tracing to the natural person level?	For corporate onboarding
Audit Trail and Reporting Exports	MAS supervisory evidence requirements	Does the platform generate exportable case records that match the evidence structure MAS expects in a supervisory review?	Yes
Model Governance and Error Rates	Regulatory quality expectations	Can the vendor provide false accept and false reject rates by document type and population?	Yes
Manual Review Quality	Regulatory quality expectations for borderline decisions	Who reviews edge cases? What is the QA process? What is the average turnaround on referred cases?	Yes
Accessibility Fallback	Consumer protection and operational resilience	What verification path is available for customers unable to complete biometric authentication?	Yes

Data Retention Configurability	Data protection obligations; MAS TRM	Can retention periods be configured by policy and jurisdiction?	Yes
Incident Response and Escalation	MAS TRM requirements for third-party risk	What happens if the verification service fails or a fraud event is detected post-verification? What is the SLA for escalation?	Yes
Explainability of Verification Decisions	MAS supervisory evidence expectations	Can the institution understand and articulate why a specific verification was accepted or rejected?	Yes
Singapore/APAC Support SLA	Operational resilience	Is Singapore-hours support available for critical issues? Is there a named point of contact for Singapore deployments?	Yes

Implementation Timeline

Institutions beginning procurement in April 2026 have approximately eight months before the NRIC authentication deadline. Vendor selection, contracting, and sandbox integration typically require four to six weeks. Technical integration and testing require eight to twelve weeks for standard deployments; longer for core banking system integrations. Parallel running and staff training require four to six weeks before go-live.

Institutions that have not commenced procurement face a material risk of incomplete migration by 31 December 2026.

The platform criteria above map to Shufti's capabilities across document verification, face verification with anti-deepfake detection certified to iBeta PAD Level 1 and Level 2, AML screening, KYB and beneficial ownership tracing, and on-premise deployment for institutions with MAS TRM data residency requirements.

Institutions can review Singapore-specific coverage, document types, and regulatory mapping before committing to a vendor decision or building and pricing a deployment plan directly without a sales engagement.

About Shufti

Singapore financial institutions need a verification platform that supports conditional routing by customer segment, integrates with Singpass and MyInfo for eligible users, handles document fallback for those without complete government-held data, meets MAS TRM data residency requirements, and generates the audit trail evidence MAS expects during a supervisory review.

Where Shufti Fits in a Singapore KYC Architecture

Singapore KYC Requirement	Shufti Support
MyInfo-eligible onboarding (SC/PR)	Singpass/MyInfo integration supporting MyInfo-based CDD workflows
FIN-holder fallback verification	Document verification and pass-based routing for incomplete MyInfo profiles
Non-resident document verification	10,000+ actively processed documents types
NRIC authentication replacement	Face Verification with anti-deepfake detection and iBeta PAD Level 1, Level 2, and Level 3 certifications
AML, PEP, and sanctions screening	AML Screening against 3500+ watchlist sources with updates every 15 minutes
Corporate onboarding and UBO verification	KYB with ACRA integration for Singapore entities; global beneficial ownership tracing
SoW evidence collection	Configurable evidence collection workflows with documented case trail and MLRO escalation
MAS audit trail requirements	Exportable case records with decision logs, screening results, and verification timestamps
Data residency requirements	On-premise and private cloud deployment options for MAS TRM localisation requirements

Certifications and Standards

Shufti holds ISO 27001:2022, SOC 2 Type II, and PCI DSS certifications. Face Verification is certified to iBeta PAD Level 1, Level 2 and Level 3 anti-spoofing standards. The platform is recognised as a DHS RIVR 2025 Top Performer, a US Department of Homeland Security programme evaluating identity verification capabilities in operational conditions.

Shufti is a technology platform, not a compliance consultancy. The platform provides the tools for verification, screening, case management, and audit trail generation that enable institutions to execute their compliance obligations. Regulatory interpretation and compliance decisions remain the institution's responsibility.

Shufti

Verify Singapore Customers Before December 2026

With eight months until the 31 December 2026 NRIC authentication deadline and MAS enforcement posture at its highest since 2023, request a demo to see Shufti configured for Singapore, including MyInfo routing, FIN-holder fallback, deepfake-resistant biometric authentication, AML screening, and MAS-calibrated audit records.

Request a Singapore KYC Demo

shuftipro.com
sales@shuftipro.com