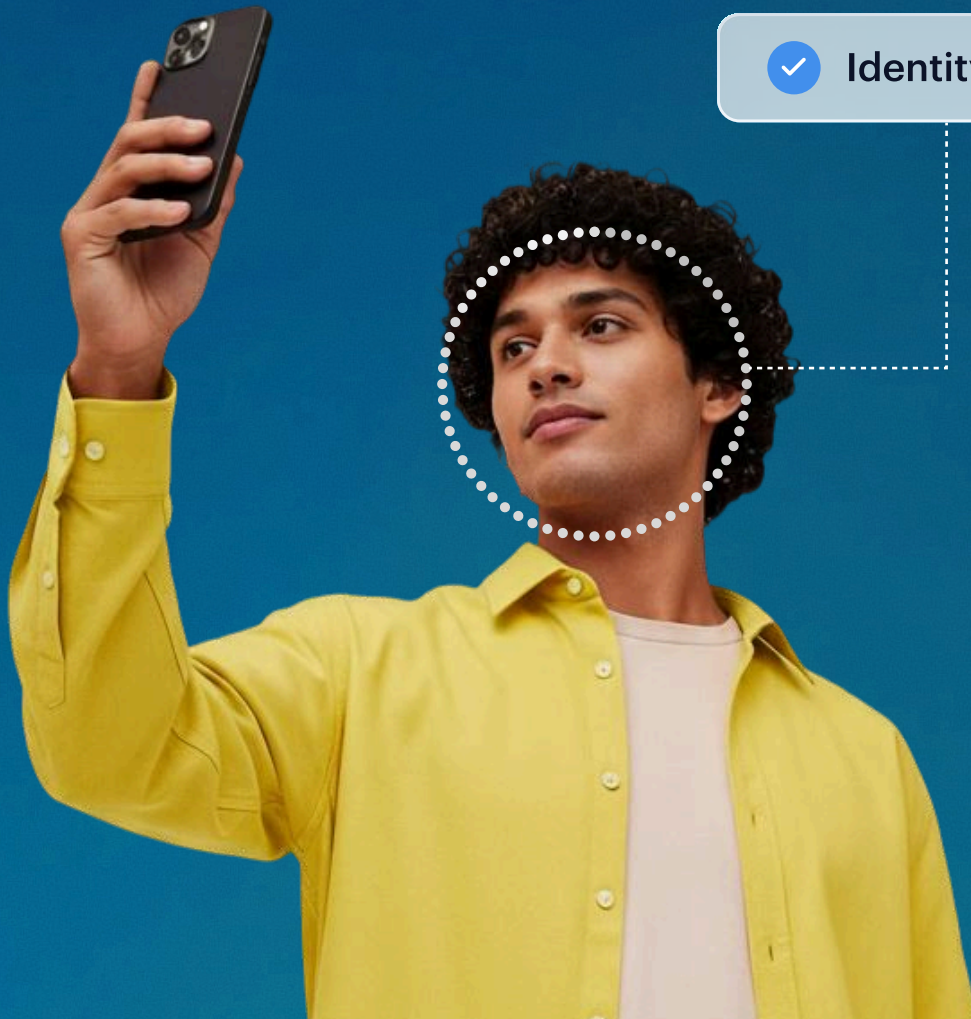


Docless KYC Verification in APAC

to Onboard more genuine users

What it is, where APAC supports it today, what the regulators permit, and how to switch without losing genuine users.



Identity Verified



KJM Age
Verification



PCI DSS



iBeta Level 3



ISO/IEC
27001:2022



CE+



QG GDPR



SOC2



GDPR



CCPA

G2 SUMMER 2026

Leader in the G2 Summer 2026 Identity Verification Asia Pacific Regional Grid Report



Recognised by Real Users. Across the Region.

Shufti has been named a Regional Grid Leader for Asia Pacific in the G2 Summer 2026 Identity Verification and KYC report. The rating is determined by customer satisfaction scores and market presence, both measured from verified user reviews.

It reflects what businesses across APAC report first-hand. Fast, compliant identity verification that works across the markets that matter, through a single integration.



Table of Contents

What's Inside

A structured guide covering the business case for Docless Identity Verification in APAC, how the three verification methods work, permitted source types by market, a practical risk routing model, enterprise verification performance, and how Shufti combines Non-Doc and document verification through one integration.

—	Introduction: why first-pass success decides the outcome	04
01	The onboarding challenge across APAC's growing digital economy	05
02	How Docless Identity Verification works: three methods	06
03	The regulatory picture across key APAC markets	07
04	Market by market permitted source types	09
05	A risk routing model for APAC onboarding	11
06	Shufti's APAC coverage: eIDV and document verification, one integration	12
07	AML and data residency alongside eIDV	13
08	Getting started	14

INTRODUCTION

Why first-pass success decides the outcome

For an enterprise, the first attempt to verify a customer is the one that matters most. When an identity is confirmed on the first pass, the customer moves straight into the product, the compliance record is complete from the outset, and the business carries none of the cost of a retry. When that first attempt fails, the effects compound. Many customers asked to try again simply leave, a manual review queue forms behind every rejected case, and the same regulatory duty has to be discharged two or three times over at higher cost.

First-pass success therefore shapes far more than the onboarding experience. It sets the conversion a business records, the speed at which compliant accounts open, and the operational load its teams carry. The question for any enterprise operating across Asia-Pacific is how to raise that first-pass rate without weakening the compliance behind it. This guide sets out how, starting with where identity can be confirmed without a document and where regulators permit it.



SECTION 01

The onboarding challenge across APAC's growing digital economy

Digital economies across Asia-Pacific are expanding rapidly. Fintech, digital banking, e-commerce, gaming, and crypto platforms are all seeing their user bases grow, and as those user bases grow, so does the volume of remote onboarding that businesses need to process efficiently and compliantly.

This growth brings a verification challenge that many businesses across the region now confront directly. Remote onboarding requires identity verification. But as the volume of users increases, businesses find that running every user through the same document-based flow creates friction that leads to avoidable drop-off, particularly among users who are low risk, digitally active, and unlikely to have a problem with a Non-Doc check.

01

Volume and velocity

As digital user bases grow, verification volumes increase. Document-based flows that work at lower volumes become conversion bottlenecks at scale.

02

Pass rate pressure

Lower pass rates mean lost customers. Users who abandon at a document capture step are rarely recovered. Every percentage point of improvement matters directly to growth.

03

One-size-fits-all verification

Applying the same high-assurance document check to every user, regardless of risk profile, adds friction where it does not need to exist.

The answer to these challenges is to make verification smarter. In many APAC markets, regulators explicitly permit Non-Doc methods for regulated onboarding, so document verification need not be the only method available, and for low risk users it need not be the first.

Businesses can choose Docless Identity Verification as the primary onboarding route for low risk users, with document verification available as the fallback where a confident match is not returned, and as the route for standard and high risk onboarding. Where regulators allow Non-Doc methods and the risk profile supports it, this approach improves pass rates and reduces the friction that costs businesses legitimate customers.

The core insight

Not every customer needs to be verified through a document. For businesses across APAC, the ability to route low risk users through Docless Identity Verification, while maintaining document verification for higher risk tiers, is what turns a compliance obligation into a competitive onboarding advantage.

SECTION 02

How Docless Identity Verification works: Three methods

Shufti's eIDV solution offers three distinct verification methods, each designed for a different assurance level and user journey. Businesses can select the right method for each risk tier, or configure automatic escalation between them.

METHOD 01

Passive Verification

Verifies user data invisibly against trusted sources, including government registries, credit bureaus, and other authoritative databases, with no friction for the user. The user provides their name, date of birth, and national identifier, and the match happens in the background. The lowest-friction method and the right starting point for low risk onboarding. Passive coverage spans 85+ countries and connects to 270+ data sources worldwide.

METHOD 02

Active Verification

Uses trusted bank or government eID logins, such as BankID, Singpass, or OneID, where the user authenticates directly through their existing credential. This provides a higher assurance level than Passive, with cryptographic assertions from the eID scheme confirming identity. Active verification is available in 40+ countries, for cases where stronger proof is required without moving to document capture.

METHOD 03

Biometrically Enriched

Adds a biometric facial match against the source photo held in the government registry or eID scheme, layered on the Passive or Active data match. The strongest assurance level within the Non-Doc flow, designed to stop fraud where a bad actor has another person's data but not their face. Configurable as 1+1 (single source) or 2+2 (dual source cross-reference) to flag synthetic identities.

85+

COUNTRIES FOR PASSIVE
CHECKS

40+

COUNTRIES FOR ACTIVE EID
LOGINS

270+

DATA SOURCES WORLDWIDE

Currency note

If a Passive check does not return a confident match, Shufti's Journey Builder can be configured to prompt the user to complete an Active eID login or a document verification step, so no legitimate user is lost to a failed Non-Doc check. The system manages escalation internally, including when a data source is temporarily unavailable.

SECTION 03

The regulatory picture across key APAC markets

Across the markets covered in this guide, regulators permit some form of electronic identity verification, and in many, Non-Doc methods are an explicitly recognised route for regulated onboarding. Several important regulatory developments have reshaped the position since late 2025.



India

India's core KYC instrument was updated on 28 November 2025. Aadhaar e-KYC remains the principal electronic verification route, with UIDAI consent required. The Central KYC Registry (CKYCRN) continues to apply for financial sector entities.



Vietnam

Vietnam phased biometric verification in July 2024 and January 2025. From January 2026, online transactions are suspended for unverified accounts; VNeID is one of three accepted channels.



China

China's KYC framework continues to evolve. Verification operates through the Ministry of Public Security resident identity card database, with regulated access through licensed third parties. Rules specific to remote, non-document onboarding remain less explicit than in the region's e-KYC leaders.



Cambodia

Cambodia's earlier position, which permitted no non-document basis for identity verification, has been superseded by the CamDigiKey national e-KYC framework. CamDigiKey now enables electronic verification for regulated businesses in Cambodia.



Japan

Japan is tightening its eKYC requirements. From 2027, the My Number IC chip is expected to become the primary electronic verification instrument, replacing a broader range of document-based eKYC methods currently permitted under the Act on Prevention of Transfer of Criminal Proceeds.

Currency note

Regulatory positions across APAC change frequently. The positions in this guide reflect verified primary source research current to June 2026. Compliance teams should verify the current position with local counsel before relying on any market specific claim for regulated onboarding.

Other key APAC markets

Beyond the markets above, the table below summarises the regulatory basis for electronic or non-document verification across the other key APAC markets in this guide. The governing instrument is named in each row.

MARKET	REGULATOR	INSTRUMENT	WHAT IT PERMITS
Singapore 	MAS	Notice 626 with Circular AMLD 01/2018	Myinfo via Singpass accepted as a reliable source for non-face-to-face CDD
Philippines 	BSP	Circular 1170 (2023) with the PhilSys Act	A PhilSys ID is sufficient proof of identity, with no additional document required
Australia 	AUSTRAC	AML/CTF regime	Identity may be verified against reliable, independent electronic data, not only a physical document
Indonesia 	OJK	POJK 8/2023	Non-face-to-face electronic customer due diligence, in practice against the Dukcapil population database
Malaysia 	Bank Negara Malaysia	e-KYC Policy Document (2024)	Fully electronic onboarding via document verification, biometric matching, and liveness
Hong Kong 	HKMA	AMLO with HKMA remote onboarding circulars (2019 to 2021)	Remote onboarding permitted, and the iAM Smart government digital ID accepted
New Zealand 	DIA, RBNZ and FMA	Identity Verification Code of Practice (2013) with EIV guidance (2021)	Electronic verification as a safe-harbour route for lower-risk customers
South Korea 	FSC	Non-face-to-face real-name verification rules (2015, expanded 2019)	Onboarding via an existing bank account and trusted databases, not only a document copy
Taiwan 	FSC	Digital Identity Verification Guidelines (2023)	Risk-based digital verification, with institutions self-assessing and adopting it. Emerging
Thailand 	Bank of Thailand	BOT e-KYC notification (2020) with NDID-based bank onboarding	Identity verified through a digital-ID platform
Bangladesh 	BFIU	e-KYC Guidelines (2020)	Paperless onboarding verified against the national NID database

SECTION 04

Market by market permitted source types

The table below summarises the primary permitted source types for Docless Identity Verification across key APAC markets. **Government rail** indicates a national digital identity system or government-operated verification mechanism. **Credit bureau** indicates that credit bureau records may be used as an identity source. **Biometric registry** indicates that biometric matching against a government registry is available or mandated.

MARKET	GOVERNMENT RAIL	CREDIT BUREAU	BIOMETRIC REGISTRY	NOTES
Australia	 DVS	Permitted	n/a	DVS is the primary government rail, credit bureau adds a practical low-risk route
New Zealand	 RealMe	Permitted	n/a	Credit bureau data permitted alongside RealMe
Singapore	 Singpass	n/a	n/a	Myinfo attribute sharing is the established eIDV route
India	 Aadhaar	n/a	UIDAI consent	28 November 2025: RBI replaced KYC Direction; CKYCR applies.
Indonesia	 NIK	n/a	KTP-el biometric	Dukcapil database access via OJK licensed entities
Philippines	 PhilSys	n/a	PSN matching	PhilSys Number (PSN) biometric matching now available
Malaysia	 MyKad	n/a	n/a	BNM eKYC guidelines govern permitted sources
Thailand	 ThaID	n/a	n/a	National Digital ID (NDID) platform for licensed entities
Vietnam	 VNeID	n/a	Mandated from Jan 2026	VNeID biometric matching now mandatory for eKYC
South Korea	 NICE	Permitted	n/a	Credit bureau eIDV well established under FSC guidelines
Japan	 My Number	n/a	IC chip from 2027	Tightening to IC chip verification by 2027
China	 MPS	n/a	n/a	Licensed third party access only
Hong Kong	 iAM Smart	n/a	n/a	iAM Smart digital identity platform for regulated businesses
Bangladesh	 NID	n/a	Biometric NID	Porichoy API provides NID verification for regulated entities
Sri Lanka	 NIC	n/a	n/a	National Identity Card registry access for regulated businesses
Cambodia	 CamDigi Key	n/a	e-KYC	CamDigiKey now enables e-KYC, prior position superseded
Pakistan	 Verisys	n/a	CNIC biometric	NADRA Verisys API provides CNIC based biometric verification

On credit bureau sourcing. In markets where credit bureau data is a permitted identity source, including Australia, New Zealand, South Korea, businesses have a well-established additional route that works particularly well for low risk onboarding. Where a user's risk profile is low and a bureau match can be returned with confidence, this route improves pass rates without requiring document capture.

Permissibility at a glance

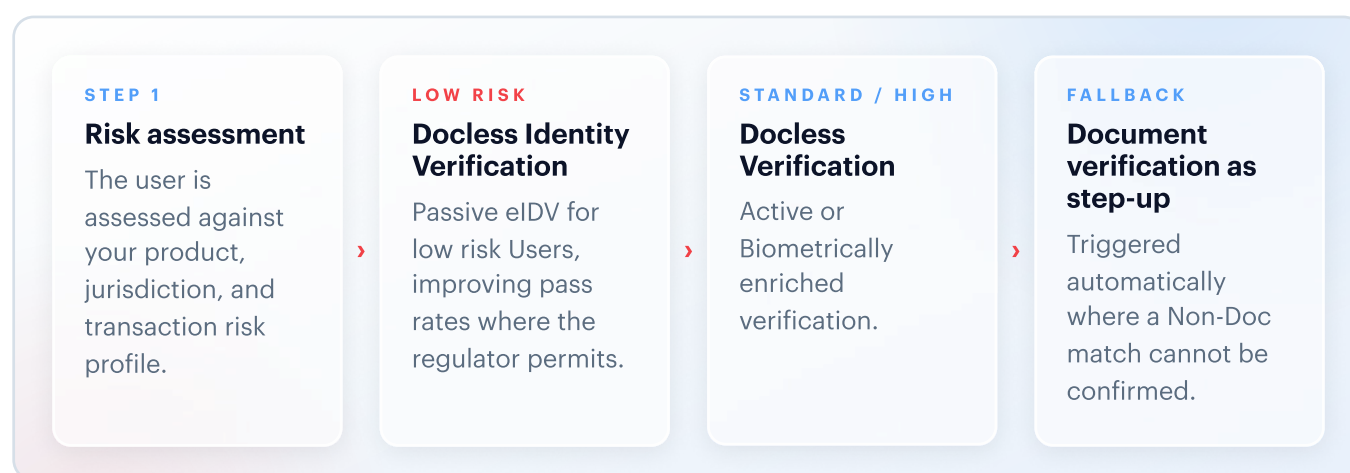
A quick reference view across all covered markets, showing which source categories are available.

MARKET	GOVERNMENT RAIL	CREDIT BUREAU	BIOMETRIC REGISTRY
Australia	● Yes	● Yes	n/a
New Zealand	● Yes	● Yes	n/a
Malaysia	● Yes	n/a	n/a
South Korea	● Yes	● Yes	n/a
Singapore	● Yes	n/a	n/a
Thailand	● Yes	n/a	n/a
Hong Kong	● Yes	n/a	n/a
China	● Yes	n/a	n/a
Sri Lanka	● Yes	n/a	n/a
India	● Yes	n/a	● Yes
Indonesia	● Yes	n/a	● Yes
Philippines	● Yes	n/a	● Yes
Vietnam	● Yes	n/a	● Yes
Bangladesh	● Yes	n/a	● Yes
Cambodia	● Yes	n/a	● Yes
Pakistan	● Yes	n/a	● Yes

SECTION 05

A risk routing model for APAC onboarding

The practical question for APAC compliance and product teams is not which method to use, but how to deploy both intelligently, routing users to the right verification method based on risk level and what regulators permit in each market. Where regulators permit Non-Doc methods and the user's risk profile is low, Docless Identity Verification can be the primary route to improve pass rates and reduce friction. Document verification serves as the fallback where a confident match is not returned, and as the route for standard and high risk onboarding.



The fallback step matters

Docless Identity Verification will not yield a confident match for every user, particularly in markets where the government rail is narrowly scoped or where the user's data does not match cleanly against the authoritative source. Shufti's Journey Builder handles this escalation automatically, so no legitimate user is lost.

Why this matters for pass rates

A business running document verification only will see avoidable drop-off among low risk users more likely to abandon at a document capture step. Deploying Docless Identity Verification for this segment, where the regulator permits and the risk profile allows, captures those users without compromising the compliance integrity of the overall flow.

SECTION 06

Shufti's APAC coverage: eIDV and document verification through one integration

What sets Shufti apart in the APAC market goes beyond eIDV coverage. It is the combination of broad Docless Identity Verification coverage and document verification across the same markets, delivered through a single integration, with AML screening running alongside both.

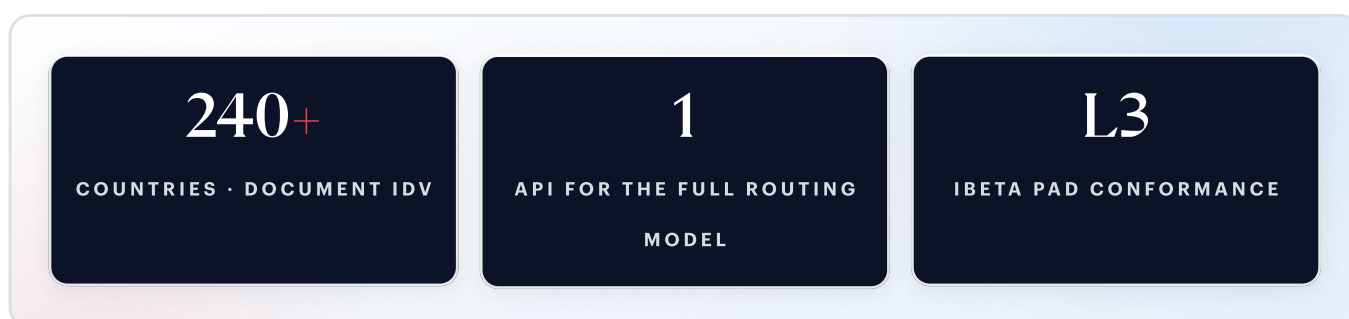
Businesses operating across APAC typically face a fragmented vendor setup, one provider for Non-Doc verification, another for document verification, and separate integrations to manage between them. Shufti removes that complexity. The full risk routing model, Passive, Active, or Biometrically Enriched Docless Identity Verification for low risk users and document verification for standard and high risk users and as the fallback, operates entirely through one API.

eIDV coverage across APAC

Shufti's Passive eIDV covers 85+ countries through connections to 270+ data sources, including government registries and credit bureaus. Active eID login is available in 40+ countries and supports APAC schemes such as Singpass, PhilSys, and iAM Smart. Where credit bureau sourcing is explicitly permitted—including Australia, New Zealand, and South Korea—businesses gain an additional low-friction route to improve pass rates for low-risk onboarding. Shufti's internal waterfall automatically escalates between eligible data sources, without requiring manual configuration for each individual fallback path.

Document verification coverage

Shufti's Identity Document Verification supports documents from 240+ countries and territories, including all markets covered in this guide. It combines optical character recognition, NFC chip reading where the document supports it, and biometric face matching with iBeta PAD Level 3 conformance, providing the audit trail, liveness assurance, and regulatory acceptance that regulated sectors across APAC require.



SECTION 07

AML and data residency alongside eIDV

Identity verification is the first gate. For regulated businesses in APAC, it does not operate in isolation. AML screening and data residency compliance sit alongside every verification decision.

AML screening

Across financial services, payments, and crypto in APAC, identity verification triggers an AML obligation. The verified identity must be screened against sanctions lists, politically exposed persons (PEP) registers, and adverse media sources. Shufti provides AML screening as an integrated component of its verification workflow, so a user verified through either Docless Identity Verification or document verification is screened in the same flow, without a separate integration. This matters particularly in APAC, where FATF's ongoing regional mutual evaluation process has placed AML compliance under increasing scrutiny across multiple markets. Businesses that can demonstrate an integrated identity and AML workflow are better positioned in regulatory conversations.

Data residency

Data residency requirements vary widely across APAC. Several markets impose localisation obligations on personal data, including biometric and identity data, that require it to be processed and stored within the jurisdiction. This applies to markets including China, India, Indonesia, and Vietnam, among others. Shufti's infrastructure supports in-region data processing for regulated markets, allowing businesses to meet local data residency requirements without fragmenting their verification stack across multiple vendors.

The practical implication. A business operating across multiple APAC markets needs a verification solution that handles different data residency regimes within a single integration. A separate vendor for each market's data localisation requirement is operationally unworkable at scale.

SECTION 08

Getting started

Running Docless Identity Verification and document verification through a single Shufti integration means no additional API work when deploying both routes. The routing logic sits in configuration, not in code.

For businesses already using Shufti for document verification

Docless Identity Verification is available as a configuration addition to an existing Shufti integration. Compliance and product teams can define the routing logic, which users go to the Non-Doc route and under what conditions document verification is required as step-up, through Shufti's Journey Builder without engineering work.

For businesses evaluating Shufti for the first time

The recommended starting point is a market specific scoping conversation. Each APAC market has different permitted source types, different data residency requirements, and different AML obligations. A scoping call with Shufti's APAC team establishes which verification routes apply for your markets, your product type, and your user risk profile before any integration work begins.

For compliance teams conducting vendor due diligence

Shufti's APAC documentation includes regulatory mapping for all covered markets, source type confirmation for eIDV coverage, and data residency architecture documentation. These materials are available on request as part of a vendor assessment process.

THE CASE FOR A COMBINED APPROACH

Docless Identity Verification reduces friction and improves pass rates for low risk users where the regulator permits. Document verification provides the assurance and audit trail required for standard and high risk onboarding. Shufti runs both through one integration, with AML alongside and deployment that meets in-region data residency requirements. No other solution in APAC combines both capabilities at this breadth.



Talk to Shufti's APAC team

Whether you are expanding into new APAC markets, adding Docless Identity Verification to an existing document verification workflow, or evaluating identity verification solutions for the first time, the right next step is a conversation.

Shufti's APAC team can map your markets, your product type, and your user risk profile to the right verification configuration, with a clear view of which source types apply and how AML and data residency requirements are met alongside.

No commitment required. No engineering work to get to a scoped recommendation.

[Schedule a demo](#)

