Azupay Financial Crimes Manual

Version 2.2 – Oct 2025

Commercial In Confidence

Version History

Version	Date	Author	Notes
0.1	25 July 2022	Mark Li	Initial draft
0.2	04 Sep 2022	Garry Clarke	Review of draft and suggested additions and edits.
0.3	15 Sep 2022	Mark Li	Updates related to feedback
0.4	23 Sep 2022	Garry Clarke	Minor edits to get to final draft state
0.5	26 Oct 2022	Garry Clarke	Update to PayTo Prohibited List – for clarity Review and edit of feedback from ELT.
1.0	07 Nov 2022	Garry Clarke	Update with extended High Risk Country List.
1.1	28 Nov 2022	Garry Clarke	Added in 2 Level Rule for Partners – see 3.1
1.2	06 Mar 2023	Garry Clarke	Added in the ability for TIP/SIP and Referring Partners to be OS based – see 2.1
1.3	07 May 2023	Garry Clarke	Change to new Azupay Branding Added in Sub-Merchant review process (from Partner Manual) and 1% Dispute Threshold notation
1.4	15 Nov 2023	Zaina Mohammed	Added in additional High-Risk Industries and increased eligibility criteria for Remittance businesses.
2.0	06 August 2024	Zaina Mohammed	Updated details of Pay-to high-risk merchants, incorporate some details from Cuscal Merchant Operations Manual V2.7 – May 2024 and review due to change of leadership team Also incorporating legal advice on the sub merchants review by Distribution partner.
2.0	08 August 2024	Michael Williams	Final Version – Approved by Senior Risk and Compliance Manager / AML & CTF Officer
2.1	26 June 2025	Michael Williams	Cash In Transit businesses added to prohibited industries.
2.2	22 October 2025	Mirjana Novakovic & Michael Williams	Inclusion of Cuscal Manual updates (issued 15 Oct) and review and build out of existing sections.

Table of Contents

1. Purpose

To provide guidance for Azupay Client onboarding requirements, risk grading and reporting obligations. This will include the minimum requirements for onboarding, KYC, ongoing monitoring and reporting processes to meet Azupay's requirements and its Banking Partner's (Cuscal) requirements.

1.1 Financial Crimes Evaluation and Guidelines

Azupay is operating in the heavily regulated financial services industry. It is governed and guided by different bodies that impose different regulatory obligations. For example,

- AUSTRAC - Australian Transaction Reports and Analysis Centre
- ASIC - Australian Securities and Investments Commission
- Cuscal (our banking partner and NPP Sponsor)

Azupay is dependent on regulated banks in Australia to access the NPP so to be successful Azupay must be mindful of the requirements placed on these banks by their regulators and their own risk appetite decisions. Azupay must fit with the risk tolerances of banks in Australia.

On top of these bodies, Azupay is required to determine and manage its own risks, apply these to its operating environment to ensure it remains a trusted, secure and financially viable business.

Azupay takes a risk-based approach to managing its customers and business, specifically to the potential of financial crime. This manual specifies what boundaries and processes are in place to ensure we achieve this goal and meet our regulatory obligations.

This document should be read in conjunction with the Cuscal Merchant Governance and Operations manual which can be located at:

https://azupayau.sharepoint.com/sites/RiskandCompliance/Shared%20Documents/General/Policies%20and%20Procedures/Financial%20Crimes%20Manual%20and%20Prohibited%20and%20High%20Risk%20List%20(Compl)/Merchant%20On%20Boarding%20Manual.pdf

2. Acceptable Clients, Industries and Minimum Standards

2.1 Check list for Organisations Azupay will do business with

Azupay maintains certain rules and standards that are required to be met for an organisation to become a client. These are as follows:

- ☐ **Not on the Azupay Prohibited List -** The client is not on the Azupay Prohibited Industries List (See below).
- ☐ **Clients with a direct relationship with Azupay -** where we charge directly for Transactions – (i.e.: Merchants and Distribution Partners, including Sub-Merchants of Distribution Partners)
  - **Australian ABN & Bank Account –** must hold an ABN and/or ACN, or an ARBN, and Australian Bank account matching their legal entity name.
  - **Australian Registered Office -** The client can be foreign owned (i.e., Australian branch of Ikea) but must have a registered office in Australia (ASIC registration) and an Australian Business Number (ABN).
- ☐ **Clients that are Referral/Integration Partners -** where Azupay has a direct relationship with the Partners Merchants (ie: Technical Integration, System Integration and Referring Partners)
- ☐ **Can be based overseas**, as long as their Merchants are domestic.
- **No Illegal Practices -** Clients must not have business relationships where you suspect that their payment products or services might be used for illegal purposes.
- **No Sanctions applicable -** Clients must not be an entity where the company, person or entity is subject to Australian autonomous sanctions or UN Security Sanctions.
- **No Complex Ownership Structures -** Clients must not have complex business ownership structure with no legitimate commercial rational.
- **Not an Unincorporated Association -** Clients cannot be an unincorporated association (a group of people working towards a common purpose without being a separate legal entity. e.g., local music groups, social groups).
- ☐ **PCI/DSS Compliant PSP's -** Card Acquiring Payment Service Providers which process, transmit or store cardholder data must only be used if they are fully PCIDSS compliant.
- ☐ **Foreign Exchange Remitter to High-Risk Destination Countries -** The client should not send funds overseas to countries that are deemed not suitable by AUSTRAC for reasons such as potential funding of terrorism. Any remitter sending funds to any of these countries will be assessed separately and will most likely not be brought on as an Azupay customer (See list of countries below).

2.2 Prohibited Industries List

In assessing a new Client, Azupay must not enter into a contract with the following prohibited industries:

Industry
Binary Options trading
Domestic/Foreign unregistered Charities
Crypto-Currency including privacy coins
CFD Trading including Crypto Trading *
Vaping equipment
Dating and Escort Services, Internet adult digital content sites and providers (MCC 7273)
Shell Banks
Online Casino's
Unincorporated Associations
Unlicensed Financial Advisors
Unnecessarily complex ownership structures (e.g., nominee or Bearer share corporations)
Products & services invoking or supporting racism, violence, abuse discrimination, hatred, terrorism, paedophilia or modern slavery.

Industry
Counterfeit/Imitation items but not limited to currency, coins, fake credentials & academic papers, stamps, counterfeiting equipment, trademark infringement items, goods infringing on 3rd party intellectual property rights
Game and hunting industries
Live animal trading
Private military companies
Arms dealers and manufacturers, weapons sellers and re-sellers, and weapons components suppliers
Blood and body parts
Other categories that we may identify in the future aligned with regulatory and industry advice • Cash in Transit Business**

* Effective 8th August 2024. **Effective 26 June 2025

2.3 PayTo – High Risk Merchants

Subject to Prior Approval by Australian Payments Plus for PayTo Product with the following MCC codes.?

- (MCC 6211) Security Brokers and Dealers
- (MCC 6530/6540) Remote Stored Value Load – Merchants
- (MCC 4829) Wire Transfer Money Orders (Cash Remitter Businesses offering cross border payment services are subject to additional conditions in addition to being registered with Austrac as a remittance service provider
- MCC (7995) Betting

Additionally, any merchant which enables an e-wallet, stored value facility, or any other liquid account for its customers is considered high-risk, regardless of the applicable MCC. These PayTo High risk merchants will require the Cuscal H risk (Appendix F) form to be completed as well as the relevant AP+ Form.

2.4 High Risk Industries

The following Client types & structures are deemed as "High Risk" and are historically prone to higher levels of chargeback, financial risk and liability as well as fraudulent activity.

In addition, entities which are beneficially owned by overseas Politically Exposed Persons (PEP's) are also considered high risk as they may be subject to influence from overseas governments. Before entering, extending, or renewing a merchant agreement, a sanctions screen must be performed against the Government by reference to DFAT consolidated list. The screening is undertaken by MVSI.

Azupay will do business with High-Risk industries, but they are assessed on a case-by-case basis.

High-Risk customer types noted below are required to be passed through for review and approval to Cuscal. This is so they can be aware of the customers that are accessing both our and their systems and services.

If there is any doubt as to whether a High-Risk client will be on-boarded or not, an initial evaluation can be requested and carried out prior to moving into the full Due Diligence and the KYC (Know Your Customer) Process.

The following lists are current as of October 2025

High-risk Merchant type/industry	Merchant Category Code (MCC)
Direct Customer of a Client which on-boards a Sub- Merchant* *(Cuscal sub merchant definition)*	No Specific MCC
Bullion dealers including gold, silver, platinum or palladium authenticated to a specific fineness. Bullion can come in the form of bars, ingots, plates, wafers or other similar mass form, and certain coins.	No Specific MCC
Buy Now Pay Later (any industry)	6052*
Business services (not classified), e.g. trusts	7399
Charities, Social Services	8398
Cigar/online tobacco seller including e-cigarettes	5993
Cyberlocker Merchants	4816
Dating and escort services	7273
Games of skill such as daily fantasy sports gaming where consumers pay a fee to enter, and the outcome of the game is determined by skill instead of luck	5816
Drugs, Drug Proprietors, and Druggist's Sundries including non-prescribed over the counter (OTC) products, e.g. vitamins, herbs and nutrients	5122, 5912
Gambling establishments including internet gambling – placing, receiving or transmitting a bet/wager **Important**: The Client MUST be registered and adhere to applicable regulations under the Gambling Sector (chapter 10) of the AML/CTF Rules & manage their risk exposure if they on-board gambling establishments.	9406, 7995, 7800, 7801, 7802
Internet adult digital content sites and providers	7273, 5967, 7841
Invoice management business, e.g. processing and collection	8931
High-risk Security Brokers and Dealers - Merchants that buy, sell, and broker high-risk securities, e.g. options	6211
Remote Stored Value Load - Merchant	6530, 6540
Miscellaneous Personal Services (not elsewhere classified)	7299
Payday lenders (Licensed)	6062*
Pubs and Clubs including membership clubs, e.g. sports, recreation, golf courses, bars, taverns, cocktail lounges, night clubs	7997, 5813
Wire Transfer / Money Order Non-Financial Institution Money Transfer *Where the Client is a Wire Transfer/Money Order / Non-Financial Institution Money Transfer provider MUST be registered with AUSTRAC and implement an AML/CTF program.*	4829, 6060*,6058*

The client needs to be in business for at least 3 years, demonstrating a stable and established presence in the industry, and must have completed at least one independent review of their AML/CTF Program in accordance with AUSTRAC requirements by an accredited independent reviewer, and without significant issues identified. In addition, they need to have a local presence and have a minimum of 100 employees.	
Skill games Merchants	7994
Direct Marketing—Travel-Related Arrangement Services	5962
Direct Marketing—Outbound Telemarketing Merchant	5966
Direct Marketing—Inbound Teleservices Merchant (Adult content and services such as website subscriptions and video streaming)	5967
Crowd Funding	No specific MCC
Subscription "Negative Option" Merchants (card absent)	5968
Airlines and Travel Agents#	4511, 4722

***Category code created by Cuscal #Azupay noted (does not require Cuscal approval)#**

2.5 High Risk Countries for Cross Border Transactions

For merchants with cross boarder exposure, additional assessment is to be conducted regarding their target customer market and destination countries. The following list is a guide to countries which are very high risk and generally unacceptable and, in most cases, Azupay's position will be NOT to transact with customers that transact with these countries:

Prohibited Country dealing list:

Prohibited countries
☐ Afghanistan ☐ Belarus ☐ Iran ☐ Iraq ☐ Korea, Dem People Rep ☐ Libya ☐ Myanmar (Burma) ☐ Russian Federation ☐ Syrian Arab Republic ☐ Yemen Rep

High-risk countries:

Critical High-risk countries	High-risk countries
☐ Central African Republic ☐ Cuba ☐ Democratic Republic of Congo – DRC ☐ Haiti ☐ Lebanon ☐ Mali ☐ Nicaragua ☐ Nigeria ☐ Panama ☐ Philippines ☐ Somalia ☐ South Sudan ☐ Sudan ☐ Turkey ☐ Ukraine ○ (PROHIBITED - Russian occupied region i.e. Crimea, Donetsk and Luhansk and Sevastopol ONLY) ☐ Zimbabwe	☐ Albania ☐ Algeria ☐ Barbados ☐ Bosnia & Herzegovina ☐ Burkina Faso ☐ Cameroon ☐ China ☐ Ethiopia ☐ Guinea Bissau ☐ Hong Kong, SAR China ☐ India ☐ Indonesia ☐ Jamaica ☐ Kosovo ☐ Morocco ☐ Mozambique ☐ Pakistan ☐ Senegal ☐ South Africa ☐ Tanzania ☐ United Arab Emirates ☐ Venezuela

Note:

- Not all countries on the list are completely prohibited, however, are on the DFAT & UNSC sanctions list or the FATF list for specific reasons. Sanctions for financing are generally targeting the enrichment of specific entities and the purpose of funds I.e., purchase of weapons hence manual assessment of the remitter is required.
- However, Azupay's position is that it will not want to deal with the sanctioned countries from a reputation & risk to the business perspective.
- Most banks have an automated system which will flag transactions to these countries for manual review and may decline the transaction based on the purpose and full customer profile.

3. Application, Assessment and Approval

3.1 Client Types and Due Diligence Required

Azupay has a risk-based approach to onboarding Merchants, Partners and Referrers. Each potential client is required to provide relevant information to enable the required Due Diligence checks to be performed and the client to be appropriately risk assessed. The extent of the Due Diligence checks is different for different types of clients

- **Merchants** – are provided a "Designated Service" (services that pose AML/CFT risk I.e., finance, digital currency, bullion dealers, gambling) by Azupay so are required to have a full Due Diligence and KYC process performed. They will be assessed for risk based on their industry, above checklist of criteria, AML/CTF requirements.
- **Distribution Partners** – are also provided a "Designated Service" by Azupay so are also put through the same criteria as a Merchant, plus Azupay needs to review the Partners' AML/CTF program documentation, as they will be onboarding merchants to provide access to the Azupay Services.

Note: 2 Level Rule for Distribution Partners - A Distribution Partner can only onboard Sub-Merchants to create a maximum of 2 levels to the transacting party. They **cannot** onboard other Payment Service Providers (PSP's) that will also onboard Sub-Merchants, as this would be 3 levels to the transacting party and would mean that Azupay would have no knowledge or visibility of the end-merchants and how they are using the Azupay Services. If 3 levels are required, the Distribution Partner, would need to become a Technical Integration Partner and the PSP would then become the Distribution Partner (so has an agreement with Azupay with the necessary protections in place) and then the Sub-Merchants can be brought on and monitored in the controlled and identified manner.

- **Referring Partner** – has no "Designated Service", so a light touch Due Diligence is performed, full KYC not required.
- **Technical Integration Partner** – is like a referring partner, with Azupay onboarding any Merchants utilising this partners system. Therefore, Azupay does not provide a "Designated Service" and these partners have a "Light Touch" Due Diligence requirement and no full KYC requirement.
- **System Integration Partners** – are like Technical Integration Partners with no "Designated Service" provided, so a "Light Touch" Due Diligence is performed, with no full KYC required.

3.2 Customer Assessment Approaches

The below shows the different types of assessments applied to the different Client Types above.

- **Light Touch** - Low risk clients which Azupay does not provide a "designated service" to. These includes Referring Partners (RP), System Integration Partner (SIP) and Technical Integration Partners (TIP) where the main commercial purpose is introducing new merchants to Azupay. Clients must complete the Azupay application:

The account manager (AM) is to notify Azupay Compliance of intent to onboard the customer, ideally when issuing Azupay Agreement. This is so the inhouse due diligence (DD) can be completed prior to receiving the signed Agreement back from customer.

- **Standard & Sub Merchants of Technical / System and Referring Partners**- Merchants which Azupay provides a "designated service" to. This will be assessed via the normal KYC onboarding process via completing the Azupay application as the first step within MVSI as illustrated in the Merchant Onboarding User Guide.

The two different DD assessments are outlined below:

o Azupay Inhouse DD
- Open-source searches on the customer & its key personnel (CEO, signatories), including social media, phone number, business website, address, ABN
- Review of Policies and AML/CTF documents provided as part of the application process. (Mandatory for Distribution Partners)

o MVSI Standard DD & KYC
- Company credit checks
- Company searches and trust deed review to identify the ultimate beneficiary owners (UBO)/s (shareholders with >25% ownership or control over the business)
- PEP & Sanctions, credit checks on the UBOs & account signatories
- Check UBO, account signatory ID with third party verification source to ensure ID details provided matches government database

These will be conducted usually without additional client involvement. Once complete the AM will be notified of onboarding decision via email and Hubspot.

- **High Risk** - Higher risk Merchant categories as per listed above in section 2.4. The High-Risk Clients will need to go through the Standard DD and KYC processes but will be more heavily scrutinised within the DD process, and maybe rejected depending on the risk profile generated from the DD process. In addition to Azupay review and approval these merchants will also require Cuscal approval.
- Some of the High risk merchant must obtain & provide to Azupay legal opinions confirming adherence with onshore/regulatory obligations as well as any licensing condition requirements before they are permitted to be on boarded with Azupay.

High Risk Clients will be required to complete enhanced due diligence (EDD); this will include completing the Azupay application and transcribing the information onto Cuscal's Customer Onboarding Form: As part of completing this form, merchants must provide the following additional information (sample):

o Sales volume
o Disputes volume and value
o Copies of business licenses authorizing customers to provide advertised products and services. Such licenses include but are not limited to:
- Medical
- Gambling
- AFSL, ACL
- Evidence of AUSTRAC valid registration as applicable, memberships of relevant Industry bodies and code of practice
- Description of their target market, jurisdictions risk and Use Cases.
- Client should also perform a review of:

o independent product review websites to identify any systemic issues with the Merchant e.g., trust pilot, productreview.com.au.
- Undertake a street view (via google maps or other application) to get comfort of the authenticity of the business operations.

The following form needs to be completed and submitted to Cuscal (merchantonboarding@cuscal.com.au) with the respective evidence for their approval.

Cuscal H Risk Merchant applications Form

Summary of Assessment Approaches

Risk	Light Touch	Standard	Higher Risk
Client Types	RP, TIP, SIP	Standard merchants	Higher risk merchants, PayFacs, Distribution Partners
Requirements	AM recommendation, inhouse DD	Inhouse DD + MVSI KYC	Inhouse DD + MVSI KYC + Cuscal EDD (Appendix F form)

Reasons for Rejection

On completion of the Due Diligence & KYC process, a report is generated by MVSI. The following are potential reasons for rejection of customer's application. The more red flags, higher the chance of rejection.

Potential reasons for rejection

- High risk industry with unusually low user reviews, repeated concerns of quality, scam, trustworthiness and overall brand image I.e., cryptocurrency exchange with frequent, loss of customer assets due to IT breach or successful hacks
- Customer found to be offering products / services prohibited by Azupay
- Unusual findings on the customer / UBO which will negatively impact Azupay's brand by association I.e., UBO known to have ties to criminal enterprises despite not legally linked on paper
- UBO sanction screening true hit with significant negative result I.e., known or suspect ties to crime syndicates and/or terrorism organisations
- High amounts of overdue debt owing by UBO & customer without satisfactory explanation
- Awareness of business being listed in industry 'blacklists'.

The reasons listed above provide an indication, but there may be other reasons for rejection that are not documented here.

MVSI Onboarding

Merchant onboarding is facilitated through Azupay's third-party provider, MVSI. Merchant applications are submitted and processed via the MVSI platform. The Sales team responsible for the customer lead is required to initiate the application within MVSI and obtain all supporting documentation necessary to complete the onboarding process.

In accordance with **Azupay's AML Program (Part B)**, the following table outlines the due diligence checks performed by MVSI as part of Azupay's merchant onboarding requirements.

Step / Component	What is Collected / Verified	How MVSI Performs / Supports Verification
Client / Business Preliminary Application	Basic business or individual data	The prospective customer fills out a form (via MVSI platform) providing legal name, business registration number / entity type, trading name, registered & trading address, etc.
Bank / Payment Details & Volume Estimates	Banking account details, anticipated transaction volumes, etc.	These are captured during the onboarding form process to help assess financial risk and validate account legitimacy.
Business / Entity Documentation	Corporate registration, incorporation documents, business license, proof of existence, etc.	MVSI requests and verifies these documents to confirm that the entity is legally registered and active.
Beneficial Ownership (UBO) & Shareholder Identity	Identity of individuals who own or control the entity (e.g. 25%+ shareholding or key controllers)	MVSI collects and verifies IDs, corporate structure, shareholding data, and resolves beneficial owners.
Identity Document Verification (KYC)	Government-issued photo IDs (passport, driver's license, national ID), address proof, etc.	Uses document verification systems, optical character recognition (OCR), authenticity checks, certificate / database checks, etc.
Screening Against Watchlists / PEP / Sanctions / Adverse Media	PEP status, sanctions lists, negative news, intelligence sources	MVSI screens submitted names (or entities) against global sanctions, PEP, and adverse media databases to flag risk.
Risk Scoring / Risk Assessment	Determine risk category (low, medium, high)	Based on submitted data, MVSI's platform assigns risk scores or triggers additional review (e.g. enhanced due diligence) for higher-risk customers.
Manual / Expert Review & Exception Handling	Cases flagged or with missing / ambiguous info	Human underwriters or compliance analysts review flagged cases or discrepancies, request further documentation or clarification.
Ongoing Monitoring / Refresh / Re-KYC	Periodic updates to identity / business information and screening	MVSI supports ongoing checks, updates, and re-verification to ensure customer data remains valid over time.

Upon completion of the review, MVSI issues a final report. The Risk and Compliance team then undertake a comprehensive assessment of the entire application to ensure full compliance with Azupay's onboarding and due diligence requirements.

If there are any exceptions, such as a PEP alert, this will be escalated to the Senior Risk and Compliance Manager for review.

4. Partners Sub-Merchants Onboarding Review Process

Azupay has a risk-based approach to onboarding Sub-Merchants in general, it understands that as part of the Partner Onboarding the Partners capabilities (eg: AML/CTF Program) have been checked and found to be appropriate for the type of Partner agreement that has been put in place. However, as part of an ongoing risk evaluation process, Azupay will need to review and approve each Sub-Merchant a Partner onboards.

The review is split into 2 based on the different types of Partner engagement Azupay has:

1. **Distribution Partner** – Where the Partner (must be registered as a Designated Service Provider) has regulatory onboarding capabilities to perform Due Diligence (DD) and Know Your Customer (KYC) activities and has an update and appropriate AML/CTF Program. With any Distribution Partner Sub-Merchant, the process of Azupay's review is split into 2 categories based on the industry that the Sub-Merchant operates in:

High-Risk Sub-Merchants – Will be reviewed in detail and in some cases Azupay will request access to the KYC documentation for that Sub-Merchant in addition the Distribution partner will need to provide information to assist with the completion of Appendix F of the Cuscal High risk merchant sub merchant form. The information is to be reviewed by Azupay prior to sign off on the sub merchant on boarding ticket. Cuscal may request review of the form and associated evidence.

High Risk Merchant and Sub merchant application form High Risk Merchant and Sub merchant form

- **High Risk Sub Merchant Review** - evidence (not an exhaustive list) of due diligence

Clients / Distribution partner must send the following documentation. This will also allow a timely response to their sub merchants onboarding review / approval. The sample list below contains details on how the documentation will be used.

- ASIC Search OR ABN Look up: To ensure company is Australian registered and it is active.
- Full KYC report including Beneficial owners: Proof of completion of appropriate due diligence.
- PEP and Sanctions screening Report: Proof of completion of appropriate due diligence.
- AFSL/ACL validation and AFCA Complaints membership: Proof of License/ registration.
- AUSTRAC Registration Remittance and Crypto: Proof of appropriate AUSTRAC registration. π
- ACMA registration Gambling: Proof of appropriate ACMA registration.
- Liquor licensing evidence
- AML/CTF program: Copy of last independent review.

- Staff criminal/police checks (where not an APRA or ASIC regulated entity))
- Copy of Employee due diligence procedure
- Flow of Fund diagram: understanding on the use of Azupay payment services.

Low and Medium Risk merchants will undergo a less detailed review, focusing primarily on a high-level assessment of the business. However, the expectation remains that the distribution partner must complete due diligence checks on all new merchants before onboarding. Azupay may request these details during the desktop review of sub-merchants, and the partner will be required to provide them.

All steps of the application review are recorded within the application for audit and record-keeping purposes. In addition, the following information is added into the Risk and Compliance Onboarding Approval form for sub-merchants;

1) Industry
2) Merchant Category Code (MCC) code

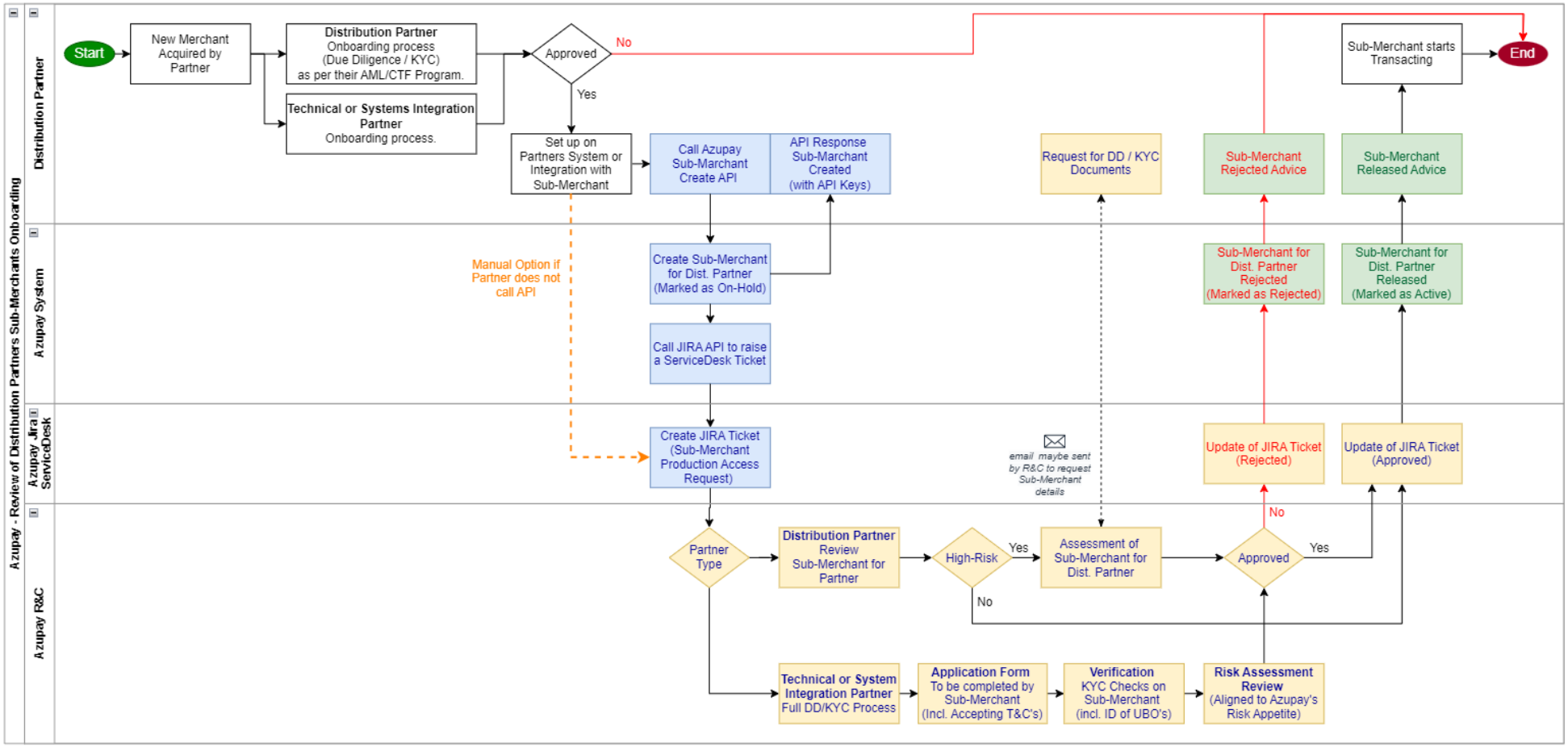
This information is essential to maintain the following;

- Merchant onboarding and due diligence
- Determining eligibility for specific payment services
- Ensuring regulatory and network compliance

2. **Technical or System Integration Partners** – Where the partner provides a platform or assists in implementing the Azupay Services into the Sub-Merchant's Platform but does not have the capabilities to perform Due Diligence (DD) and Know Your Customer (KYC) activities. For these Partners Azupay will perform the full regulatory required DD and KYC process as it does for its direct merchants.

   The review process will be part of the configuration process of the Sub-Merchant onto the Azupay System, using either the Client Creation API or a specific category of Help Desk Ticket. This will process is conducted in the back office of Azupay and will not overtly effect the set up or configuration of the Partners Sub-Merchant on the Azupay System.

The next few pages shows a visual representation of the flow and technical interface with Azupay.



Sub-Merchant Request (Blue Boxes)

The Diagram above shows how a Partner has the option to call an API to automatically create a Sub-Merchant within the Azupay System.

See the links to the Sub-Client creation information and the Client API specifications in the Azupay Developer Portal.

- Information - https://developer.azupay.com.au/guide/sub-clients.html
- API Specifications - https://developer.azupay.com.au/api/#tag/Clients

This API call will create the Sub-Merchant (Client) in a disabled state. It will also automatically create a Jira ServiceDesk ticket to enable the "Sub-Merchant" to be reviewed internally by Azupay. (See the Blue Boxes in the diagram).

Alternatively - The Partner can raise a ServiceDesk ticket of the specific type "Sub-Merchant Production Access Request" and enter the required details of the Sub-Merchant. (See the orange line and text in the diagram).

ServiceDesk link is - https://azupay.atlassian.net/servicedesk/customer/portal/3

Risk & Compliance Review (Yellow Boxes)

Risk & Compliance will respond to this Ticket and based on the type of Partner making the request, will perform the appropriate review required

- For a Distribution Partner
  - Azupay will do an initial review to decide if this Sub-Merchant is High-Risk or not, or if this Sub-Merchant has been previously off-boarded from Azupay Services.
  - If not High-Risk and not previously off-boarded - the Sub-Merchant is immediately approved - via the update to the Ticket.
  - If it is High-Risk or previously off-boarded - it is assessed (which may include requesting to see the Sub-Merchants DD/KYC information from the Partner). This assessment decides whether this Sub-Merchant is Approved or Rejected, and the Ticket is updated accordingly.
- For a Technical or System Integration Partner
  - Azupay will perform the full DD/KYC process with the Sub-Merchant with the following steps
    - Application – Sub-Merchant Complete an online application form that includes acceptance of Azupay T&C's
    - Verification – KYC checks that include the identity verification if the Ultimate Beneficial Owners (UBO's) of the Sub-Merchant organisation.
    - Risk Assessment Review – A final review by Azupay of the details of the DD/KYC process assessing the risk profile of the Sub-Merchant compared to Azupay's risk appetite (See section 2 of this document).

The end result of both these processes is either an Approval or Rejection of the Sub-Merchant for use of Azupay Services.

Approved / Rejected (Green Boxes)

If Approved the Sub-Merchant will be created on the Azupay System in coordination with the Partner and is made available to use the Azupay Services.

If Rejected the Sub-Merchant is marked as rejected.

If Approved or Rejected - the Partner is advised accordingly via the ServiceDesk ticket notification.

5. Ongoing Monitoring & Reporting of Distribution Partner Obligations

The distribution partner must undertake ongoing monitoring and/or regular reviews of approved merchants based on risk rating and/or any changes to regulatory or compliance requirements (e.g., changes to AML/CTF regulations). Azupay requires our distribution partners to implement ongoing sub merchant monitoring processes as detailed below. Distribution partners will need to be registered and or enrolled with Austrac. They will need to meet their own regulatory obligations.

5.1 New Merchants

The distribution partner must monitor their new merchants, especially in the first three months of operation, to recognise any unusual behaviour or excessive payment disputes. The Distribution partner should identify and investigate any of the following unusual/adverse behaviours:

- Unusual variation in settlement value or in transaction mix or from turnover stated in application.
    - High frequency of declines, refunds, or payment disputes.
- Trading outside stated business hours.
- Nil or very low activity compared to that stated in application, which may indicate that there is a sleeper Merchant.
- Changes in business profile (location, principals, bank account details, type of products/ services etc.)

As part of our Ongoing Customer Due Diligence (OCDD) procedures, Azupay will periodically and randomly select sub-merchants of each Distribution Partner to verify that KYC information has been properly collected and verified.

5.2 Ongoing Merchant Transaction Monitoring

The distribution partner must monitor each of its merchant's activities on an ongoing basis to detect fraud or other wrongful activity. At a minimum, the distribution partner must monitor for the below listed type of activities:

- Fraud and scams committed at a Merchant, including high levels of disputed transactions.
- Clients should:
- Be aware of scam typologies (www.scamwatch.gov.au).
    - Have increased monitoring of inbound transactions of Merchants who are particularly targeted by / preferable to scammers.
    - Have the capability to hold funds if they suspect a scam.
- High level of complaints and/or adverse product/service reviews, including reviews of reputable review websites such as au.trustpilot.com and productreview.com.au.
- Changes in operations, including anomalies in individual transactions.
- Transactions with abnormal patterns, including high velocity events.
- Behavioural patterns vary from historical transactions.
- Linked transactions/network patterns, such as refunds,
- Partners must have a process in place to fulfill their reporting obligations if registered with AUSTRAC, as outlined in their AML & CTF program. Clients are responsible for reporting any suspicious transactions to AUSTRAC. However, Azupay acknowledges that specific details cannot be disclosed due to tipping-off provisions."

- Partners is also expected to have a process around screening (including employee) and a retention policy for all key documentation including KYC documentation, transaction monitoring and complaints.

Distribution Partners must take prompt action to investigate any risk or compliance matters, including from its transaction monitoring within 72 hours. Partners must take immediate action to suspend merchant activities where there is a confirmed material adverse event including

- breach of scheme requirements or any law,
- fraud/scams outside of appetite,
- insolvency event.

The obligation is on the distribution partner to immediately report to Azupay designated. contact any:

- Suspected fraudulent or criminal activity identified within the sub merchant base.
- Merchant activity that places the distribution partner at risk as per the Azupay merchant service agreement
- In the event of repetitive fraud, Azupay has the right to ask the partner o provide evidence of their fraud oversight program and procedures to mitigate and prevent such activities.

5.3 Ongoing Due Diligence

The partner should review their Merchants on a periodic basis as per the recommended time frames or upon a specific Azupay request:

- High Risk - Every 12 months.
- Medium Risk - Every 1-2 years.
- Low Risk - As may be required, or in the event of (e.g.) change in Merchant ownership, including "Know Your Customer" (KYC) identification, verification of identity and ongoing customer due diligence.

These reviews should also include:

- Business structure, including legal entity type, e.g., change from sole trader to
- partnership, company, or trust.
- Business financials, change in goods and/or services sold.
- Ownership, e.g., sale of a business, mergers, owner deceased and business
- assets subject to probate, etc.
- Change in directors (added or removed) of a Merchant

5.4 Reporting Obligations

The partner must conduct ongoing monitoring and annual reviews of their sub merchants. Some of the key data points would be:

- Number of new onboarded Merchants.
- Number of declined applications.
- Number of high-risk Merchants who have been subject to appropriate enhanced due diligence
- Number of off-boarded Merchants e.g. due to fraud, on-compliance etc.
- Overdue Merchant on-going due diligence.
- Number and nature of customer complaints
- Number of Suspicious Matter Reports lodged.

As part of the partner's annual OCDD they will be required to submit a report on the specified data requirements for the sub-merchants onboarded.

6. Azupay Ongoing Monitoring & Reporting

6.1 Transaction Monitoring

In accordance with the Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) Act 2006 (the Act), Azupay has implemented a robust transaction monitoring (TM) system through third party partner Comply Advantage (CA). Customer transaction data are fed through CA and will trigger alerts for review. Azupay monitors the transactional behaviour of its merchants' clients in addition to our merchants' transactions. To ensure appropriate rule-sets and thresholds are applied, customers are assigned risk levels of Low, Medium, or High. This approach enables the effective analysis of transactions and supports the detection of unusual or suspicious activity. The transaction monitoring process applies to all transactions processed via PayID, PayOut & PayTo and client top-ups/sweep of settlement accounts for all customer types.

Service Level Agreements

Customer Risk Level	Service Level Agreement	Description
High Risk	**24 hours**	Customers with significant risk factors. Examples: Complex ownership structures, high velocity of inbound and outbound transactions, high value transactions
Medium Risk	**24 hours**	Customers with some risk indicators that warrant closer monitoring. Examples: higher transaction volumes or customers in moderately higher-risk industries.
Low Risk	**24-48 hours**	Customers with minimal indicators of financial crime risk. Examples: standard retail clients with clear transaction histories.

Review occurs post transaction with soft stops being placed, resulting in no customer impact.

The TM review process occurs daily (business hours) and is managed by the Risk & Compliance department.

Currently we have an in-house tool that monitors the PayTo / mandate creations and transactions.

Alert Management

The transaction monitoring process is outlined in the format presented below.

1. **Generation**: The system generates alerts through batch processing. Transactions cannot be intercepted in real time; therefore, reviews are conducted post-initiation.
2. **Triage**: Initial review is conducted to determine the hit ratio against the rule segment and prioritization.
3. **Investigation**: Customer profile review, transaction pattern analysis and obtain clarification and explanation from merchant/customer.
4. **Escalation**: If suspicion cannot be reasonably dismissed, escalate to the Financial Crime Manager for further review.
5. **Closure**: If no suspicion, document rationale and close the alert/case.

The reference to triaging, remediating and investigating an alert/case can be found in the ComplyAdvantage Transaction Monitoring and Screening guide. Refer to pages 35-39 for Alert View and pages 60-62 for Case View.

Azupay has implemented keyword monitoring to identify specific terms within transactions that may indicate potential risk. When triggered, these keywords initiate a review and any necessary follow-up actions to determine whether further investigation is required. This screening process is managed through JIRA, ensuring that all alerts are tracked, reviewed, and resolved in accordance with Azupay's financial crime compliance procedures.

Detection Scenarios & Red Flags

- Rapid movement of funds in and out of accounts with little or no business purpose.
- Structuring/smurfing of transactions.
- Rapid movement of funds in and out (velocity).
- Transactions inconsistent with the customer's business, profile, or historical activity.
- Use of multiple accounts or services under a single customer profile.
- Repeated use of top-ups, PayOuts, or PayTo transfers inconsistent with declared activity.
- Frequent use of refund or reversal mechanisms.
- Repeated alerts for keyword triggers
- Use of multiple accounts to obfuscate funds flow.
- Lack of clear or verifiable source of funds or wealth.
- Discrepancies between transaction data and customer information (e.g., mismatched names)

To ensure compliance, these red flags are:

1) Configured within the Comply Advantage, QuickSight and JIRA systems.
2) Regularly reviewed and updated in line with regulatory guidance from AUSTRAC or equivalent authorities.
3) To trigger further investigation workflows for escalation, documentation, and potential Suspicious Matter Reports (SMRs).

When suspicion is formed on a merchant based on account behaviour, customer profile and red flags, a suspicious matter report (SMR) will be lodged with AUSTRAC.

6.2 Fraud and Dispute Monitoring

An effective fraud and dispute management process is an integral part of fighting financial crime, protecting our customers and Azupay's reputation. This is covered by two methods and handled by the Risk & Compliance team, usually reviewed on a T+1 basis.

1. NPP Disputes & Investigations
   The primary source of queries and investigations, this is performed via https://www.cuscalpaymentshub.com.au/cuscal-home/#/home
   When a fraud / investigation via the NPP platform is raised by a counterparty bank (usually by a customer), the counterparty bank sends a message with relevant information to Azupay to initiate an investigation. This is usually a request for fraud investigation or information relating to certain NPP transactions. Here's a step-by-step example that will apply in most cases.

2. IREC Indemnities for Action
   These are emails from Cuscal calldirect@cuscal.com.au and are non-NPP scams. The attachments include a formal letter from requesting return of funds due to a scam, at this stage the OFI appears to be the only counterparty bank involved. The transactions are often of smaller value, sent via OFI bank transfer / RTGS to our customer's Cuscal account, where they are swept to the settlement account. Much of the same from NPP fraud applies with results being advised to by OFI

Note: Abnormal volume of disputes may result in termination of Merchant facilities and subsequent offboarding with Azupay. It may also result in the customer's details being shared with industry blacklists.

Azupay currently has a 1% threshold of disputes to transaction ratio. If this threshold is breached, Azupay will communicate with the Merchant or Partner to work through any issues or resolutions with an aim to reduce disputes and remain under the threshold.

Azupay will continue to monitor the ratio over a short period If the threshold continues to be breached then the termination of the agreement with the Merchant or Partner is likely.

This threshold may vary for certain Merchants or Partners depending on volumes of transactions and determined acceptance limits of disputes with that specific Merchant or Partner.

6.3 Suspicious Matter Report

If we suspect that a person or transaction is linked to a crime, it must be reported to the Risk & Compliance team where it will be assessed. If suspicion is formed, a SMR is required to be sent to AUSTRAC. SMRs help protect Australia against money laundering, terrorism financing and other serious and organised crime. They are also an important part of our AML/CTF reporting obligations and is done via https://online.austrac.gov.au/ao/login.seam.

SMRs apply not only to suspicious transactions, but also actions & behaviours of individuals. This includes customers and employees of Azupay. If any such actions are witnessed by Azupay staff, the Risk & Compliance team are to be notified, along with details to decide on whether the actions warrant submitting an SMR.

Azupay will investigate and collate transactions information from merchant. As in most instances the suspicious transactions relate to the merchant's customer rather than the merchant itself. Fin crimes manager will discuss cases with manager prior to submission.

Deadline for reporting terrorism related events is 24 hours from formation of suspicion. All other events are 72 hours.

7. Azupay Ongoing Reviews Merchants

7.1 Customer Periodic Review

To ensure Azupay customers are consistently assessed at an appropriate risk level, periodical reviews are performed based on existing risk grades:

High Risk	Every 12 months.
Medium Risk	Every two years.
Low Risk	Every five years or as may be required, or in the event of (e.g.) change in merchant ownership, including "Know Your Customer" (KYC) identification, verification of identity and ongoing customer due diligence.

Our third-party provider, MVSI will confirm any changes to customer's key personnel, business structure before conducting credit checks, company searches, PEP & Sanction checks on the merchant UBO and directors. This will generally conclude in the background without involvement from the merchants.

In the event where a company search reveals a match MVSI will note an exception flag for Azupay R&C team investigation and resolution. Any new PEP's identified as part of the OCDD program will require notification to Senior Manager risk and compliance who will seek Management approval. Where there is changes to company structure such as Beneficial owner information or director changes merchant may be required to re undergo KYC KYB check. For changes such as addresses these will be collected from the merchant and verified against a new ASIC Company search.

OCDD Activity	Description	Key Details / Actions
Data Validation and Record Review	Ensures all customer and business information remains accurate and up to date.	Verifies KYC and KYB records - Confirms identity documents, beneficial ownership, and business registration details.
Sanctions and Watchlist Screening	Screens customers against domestic and international sanctions lists.	Checks AUSTRAC, DFAT, OFAC, and UN sanctions lists - Flags any positive or potential matches for manual review.
PEP (Politically Exposed Persons) Checks	Identifies customers or beneficial owners who hold prominent public positions or present higher risk.	Screens for PEP status - Initiates Enhanced Due Diligence (EDD) where PEPs are identified.
Adverse Media Screening	Detects reputational or financial crime risks through automated adverse media searches.	Scans global databases for negative news, fraud, or criminal activity associated with customers or entities.
Trigger-Based Reviews	Conducts additional checks when risk triggers occur.	Triggered by changes in ownership, transaction behaviour, or regulatory updates - Initiates review and re-verification as required.
Reporting and Documentation	Provides Azupay with a detailed summary of OCDD findings.	Delivers a comprehensive report outlining verification results, exceptions, and recommended actions - Reviewed by Azupay's Risk and Compliance team for final assessment.