Third Party Onboarding Due Diligence Questionnaire

PURPOSE

Payments NZ's API Centre works with the Industry to create the open banking standards and protocols needed for payments initiation and account information to ensure fast, secure, user-friendly data sharing for New Zealand.

The purpose of this questionnaire is to capture as much of the base information as possible that an API Provider may need to enable it to undertake due diligence as part of its partner onboarding processes (and to reduce the level of duplication involved when a Third Party needs to supply similar information to multiple API Providers).

Each API Provider will undertake its own independent assessment of responses and may have follow up questions depending on the answers provided. An API Provider may also have its own independent requirements and will communicate these separately.

DISCLAIMER

Payments NZ does not make any warranty, guarantee or representation, regarding the Questionnaire, or any information provided in connection with the Questionnaire. Neither Payments NZ, nor any of Payments NZ's directors, officers, employees, contractors, staff, agents, or other representatives shall be liable to any person, for any loss, damage, cost, charge, expense or liability, incurred or sustained by that person arising in any way out of, or in connection with, the Questionnaire or any information provided in connection with the Questionnaire.

CONTENTS

GUIDANCE

How to Complete

All tabs included in this questionnaire require your attention. Please ensure you complete all required sections.
Please use the latest version of this template which you can access through https://www.paymentsnz.co.nz

Supporting Documentation

Some questions will require you to submit supporting documentation as evidence. Please use the 'Supporting Documentation' tab to attach or link to the relevant materials and refer to the appropriate document by name in your answers. For highly confidential documents you may choose to provide only a cover page, or encrypt the document and provide passwords to recipients directly.

How to Submit

Once completed, the questionnaire should be uploaded to your bank partner.

VERSION
Version 1 - August 2022 - Drafted with support of EY New Zealand

ABOUT YOUR ORGANISATION

Purpose
These questions allow the API Provider to understand your organisation's identification and history.

Q#	About your Organisation	Your Answer
1	Legal / Registered Company Name	ABC Co Insurance Limited
2	Registered company address	1 Street, Suburb, Auckland, New Zealand
3	Does your organisation have a RealMe or Green ID Verification?	Yes
4	Please provide more information about your organisation, including: legal status (e.g. company, trust, partnership), place/country of incorporation, corporate and ownership structure, and any trading names used by the organisation.	Company, incorporated in New Zealand, ABC Co
5	Please provide your organisation's NZBN	9684631450985
6	Please provide your organisation's GST number	124-746-986
7	Please confirm your organisation has bank accounts in New Zealand	Yes
8	Please provide/attach a list of directors of your organisation, including contact details (email, phone)	See attached
9	Please provide/attach details of the executive officers of your organisation (name, role, email).	John Doe Director of ABC Co john.doe@abc.co.nz
10	Please provide details of the Accountable Person for your use of APIs. Provide their full name, role, email, role description.	Paul Smith CTO paul.smith@abc.co.nz Paul has been with the organisation for 10 years and is responsible for all technology service delivery functions.
11	Please provide your organisation's Website Address	www.example.co.nz

3a	Please provide details and verification number	RealMe ID 185739

Q#	About you - the primary contact person	Your Answer
12	Full Name	Joe Bloggs
13	Role	Open Data Lead, Enterprise Technology
14	Phone Number	+64 21 647 986
15	Email Address	joe.bloggs@abc.co.nz

Q#	Organisation History	Your Answer
16	Does your organisation hold any NZ Financial Services licences or registrations?	Yes
17	Has your organisation, or any director or senior managers ever been the subject of any investigation, enhanced regulatory monitoring, informal or formal enforcement action from the RBNZ, FMA, Privacy Commissioner, Commerce Commission, trustee supervisor, applicable Registrar or other regulator/supervisor known to them? In addition, have you ever corresponded with your regulator, and your regulator has come to the view that you have committed a breach? Further, has your organisation, or any director or senior managers ever been declared insolvent or bankrupt? If yes, please provide further details / attachments.	No

16a	Please provide details and a copy	We are a Registered Insurer (please find attached copy along with this file)

18	Does your organisation comply with the Financial Service Providers (Registration and Dispute Resolution) Act 2008?	Yes			
19	Is your organisation part of an approved dispute resolution scheme?	Yes	**19a**	Is it one of the following approved DR schemes? - Banking Ombudsman (BOS) - Insurance and Financial Services Ombudsman (IFSO) - Financial Services Complaints Ltd (FSCL) - Financial Dispute Resolution Service (FDR)	Yes, IFSO and FSCL
20	Is your organisation an AML / CFT Reporting Entity?	No	**20a**	Please advise of the process, systems and controls you use to manage your exposure to AML / CTF risk.	
21	What applicable insurance cover does your organisation have? Such as: - Public Liability - Professional Indemnity - Crime and Fidelity - Privacy and Security Protection (Information Security) - Cyber - Payments and Fraud Protection - Statutory liability - D&O and legal costs for directors - Material damage or business interruption Please attach details	Yes, see attached description of cover			

ABOUT YOUR USE OF APIs

Purpose
These questions aim to provide the API provider with information on the service your organisation will provide and how your organisation will use the APIs.

Q#	About your Organisation's Service Offering	Your Answer			
1	Does your organisation intend to use: a) account information API and/or; b) payment services API	a) and b)	**1a**	Please describe intended use	For details on planned use of API please see attached 'XYZ Banking integration User Journey Summary.pdf'. Account information will be a core service for all users, while payments initiation is an additional option.
2	Do you intend to use any other API(s)?	No			
3	Please provide/attach a summary of the intended use case(s) of the API(s) selected i.e. the service you are offering to your customers.	Data mine bank transaction behaviour data of our customers to offer discounted insurance quotes.			
4	Has your organisation previously established API connectivity with any other NZ Banks or International Banks?	Yes - NZ banks	**4a**	Please describe current status and usage with supporting evidence	We have an existing API connection with ABC Bank in NZ which is not part of the API Centre
5	Has your organisation completed a Proof of Concept or testing with the API Centre sandbox and now ready to progress to production verification testing?	No	**5a**	What is your expected timeline to be ready?	This is in progress, approximately 3 months
6	Do your organisation's solutions fully comply with the Payments NZ API Standards?	No	**6a**	Please explain any variations	Our solution has been designed and developed according to the standards. Assurance testing is in progress.
7	Please specify whether your organisation intends to use any of the below authentication methods and please explain if any variations between account information and payment.				
	a) Browser based redirection	Yes	**7a**	Please explain variations if any	Note Payment Initiation n/a for our use case
	b) App based redirection	No			
	c) App to browser redirection	No			
	d) Brower to app redirection	No			
8	What types of devices and operating systems will your organisation support? Please provide evidence where relevant.	Generic PC - Windows 10 Apple iPhone - iOS 14, 15, 16 Google Pixel - Android 11 & 12 Attached example screenshots from early system test cycle			
9	What is your organisation's approach to error handling, where not prescribed by the standards?	Failures in API calls and high error rates are monitored in manual queues by our IT support desk to resolve within certain SLAs			

Q#	About your Organisation's Service Delivery Model	Your Answer
10	What are your organisation's forecast API volumes and how are they mapped to technology and service model capacity planning, performance SLAs, and customer / partner SLAs? Please attach	See attached

11	Will you share data sourced via the APIs with any related organisation including subsidiaries, joint ventures, or parent company, or with any other organisation?	Yes	**11a**	Please explain in detail.	
12	Please provide details if any data, sourced through the APIs, will be stored, processed or accessed outside New Zealand?	N/A			
13	Please provide/attach details, including relationship boundaries, of any technical service providers who will manage, secure, store or otherwise have access to the data obtained through the APIs.	N/A			
14	If your organisation conducts any form of outsourcing related to the API model (including a Technical Service Provider), is there an appropriate service level agreement and business continuity plan in place? Please attach any relevant documentation.	N/A			

ABOUT YOUR APPROACH TO RISKS

Purpose
These questions allow the API Provider to understand your organisation's approach to risks, including your organisation's approach to Information Security for your API solution.

Q#	Approach to risk management	Your Answer
1	Please describe your organisation's approach to risk and compliance management, including frameworks, governance models, policies and roles and responsibilities. Please attach supporting documentation to fully explain.	Please see attached slides outlining risk within the organisation

Q#	Approach to Information Security for your API solution	Your Answer
2	Please provide details (including copies) of any formal security qualifications / certifications held by your organisation, including but not limited to: -ISO 27001 / 2, -SOC 2, -ISAE 3000, -SAE 3150, -PCI DSS Please specify if any qualifications / certifications are self-certified or externally audited.	Yes
3	Please describe the security aspects of your organisation's solution. You may wish to include the following elements listed below. Documents may be attached to cover multiple areas for simplicity. -Data classification and handling -Secure-by-design methodologies including security scanning, hardening or other automated tools -Vulnerability Management -Testing and Release Management -Data storage and transmission controls including use of on-prem, public or private cloud. -Physical, procedural and technical admin access controls to customer data including privileged accounts -Real-time monitoring for incidents -Activity, event and security logs -Staff security training -Firewall and perimeter defence including DDOS -TLS and certificate management -Information Security Operations management and Incident Management procedures. -Performance and Capacity management -Data back-up and restoration -Compliance with privacy laws and regulations -Business Continuity and Disaster recovery plans	Please see attached document 'NZ API Standards Security Assessment_Final_Aproved'

2a	Please state what current certifications or standards are applicable for your solution and attach evidence.	We maintain an information security policy in alignment with ISO27001

SUPPORTING DOCUMENTATION

A - ABOUT YOUR ORGANISATION

Q#	Document required	Document Guidance	Attached?	Attached document name (s)
8	List of directors	This can be a PDF copy of your organisation's Company Extract available at https://companies-register.companiesoffice.govt.nz/	Yes	*Company_Extract_ABC Co_2022*
9	Executive officers details	This can be in any format e.g. Excel, Word, PDF, PowerPoint	Yes	*Executive Officer Details 04.06.2022*
16	NZ Financial Services licenses or registrations	PDF copies of applicable licenses or registrations	Yes	Insurer_License_v3.2
17	Fit & proper related documentation	PDF copies of applicable documents	N/A	
21	Details of applicable insurance cover	PDF copies of Certificates of Insurance and/or any other relevant documentation	Yes	*Insurance_Cover_Documentation_2022*

B - ABOUT YOUR USE OF APIs

Q#	Document required	Document Guidance	Attached?	Attached document name
3	Supporting documentation of intended use case(s) of the API(s) selected	PDF copies of applicable documents	Yes	*Intended use case.pdf*
4a	Evidence of successful API integration	PDF copies of applicable documents	N/A	
8	Examples of operating systems and devices that you will support	This can be a screenshot of system test cycles or any format e.g. excel, word, pdf	Yes	*Screenshot18.06.2022*
10	Details of API forecast volume and mapping	PDF copies of applicable documents	Yes	*Volume and Mapping.draft1*
11	Details of sourced data shared with any other organisation	PDF copies of applicable documents	N/A	
12	Details of data stored, processed or accessed outside New Zealand	PDF copies of applicable documents	N/A	
13	Technical service provider details	PDF copies of applicable documents	N/A	
14	Service level agreement / business continuity plan	PDF copies of applicable documents	Yes	*Standard Customer SLA.pdf, BCP May 2022.pdf*

C - ABOUT YOUR APPROACH TO RISKS

Q#	Document required	Document Guidance	Attached?	Attached document name
1	Risk and compliance management	This can be in any format e.g. Excel, Word, PDF, PowerPoint	Yes	*ABC Co risk slides_2022.ppt*
2	Applicable security qualifications / certifications	PDF copies of applicable documents	Yes	*InfoSecPolicy_cert.pdf*
3	Applicable security related documents	PDF copies of applicable documents	Yes	*NZ API Standards Security Assessment_Final_Aproved*