Publication Date: 14 December 2021

Open API Framework for the Hong Kong Banking Sector

Common Baseline

The Hong Kong Association of Banks

Introduction to the Common Baseline

Background

The HKMA's Open API Framework for the Hong Kong Banking Sector dated 18 July 2018 (the "**HKMA Open API Framework**")[1] sets out the HKMA's policy objectives for the development of API for the Hong Kong banking industry, specifically to:

1. ensure the competitiveness and relevance of the banking sector;

2. provide a secure, controlled and convenient operating environment to allow banks and their third party service providers ("**TSPs**") to work together and develop innovative/integrated banking services that improve customer experience; and

3. keep up with international developments in the delivery of banking services.

The HKMA Open API Framework states that the HKMA has taken note of the mandatory approach to API adoption in the banking sector adopted by some jurisdictions such as the EU, the UK and Australia, but notes that the HKMA:

1. has decided that a collaborative and phased approach is an appropriate approach for Hong Kong; and

2. will monitor the progress of Open API implementation in Hong Kong and consider the need for new regulatory measures if necessary[2].

It follows that rather than implementing a centralized model of API regulation, under which banks and collaboration partners alike are regulated and subject to mandatory standards, the HKMA has communicated its expectations that banks should do the following in relation to each API collaboration with third party service providers ("**TSPs**") accessing Phase II APIs (Subscription and new applications for product/service), Phase III APIs (Account Information) and Phase IV APIs (Transactions):

1. carry out onboarding checks on TSPs;

2. conduct ongoing monitoring of TSPs; and

3. enter into a bilateral contractual relationship with each TSP.

The specific areas for onboarding checks and ongoing monitoring of TSPs and the collaborations between banks and TSPs are set out in the CB Requirements (as defined below).

The Common Baseline is intended to facilitate and streamline banks' onboarding of TSPs. As elaborated in the HKMA Open API Framework, the Common Baseline is a list of questions and requirements addressed to business and risk management considerations, including customer protection measures (see below for more details), with the overall objective of ensuring that the requirements for onboarding TSPs are **fair and reasonable and commensurate with the risks involved**[3]. The Common Baseline sets out the expectations in relation to accessing Phase II, Phase III and Phase IV APIs.

Should TSPs or prospective TSPs wish to seek supervisory feedback from the HKMA on Open API matters, they are most welcome to directly approach the HKMA's Fintech Supervisory Chatroom.

---

1 https://www.hkma.gov.hk/media/eng/doc/key-information/press-release/2018/20180718e5a2.pdf
2 Paragraph 8.2 of the HKMA Open API Framework.
3 Paragraph 41 of the HKMA Open API Framework.

Approach to the Common Baseline

According to the HKMA Open API Framework, the specific business and risk management considerations that should be incorporated into the Common Baseline are the following:

1. **Business** – including financial soundness, reputation, quality of management and appropriateness of business operations; and

2. **Risk management** – including capabilities and controls of the TSP in the areas of risk management, business and technical expertise in the field, customer and data protection measures (including the avoidance of the collection of excessive personal data), cybersecurity and IT controls (including, among others, confidentiality, integrity and availability, monitoring and migration measures and contingency planning).[4]

The Common Baseline organises these considerations under seven topic areas (the "**CB Requirements**"), each of which draws from legal and regulatory requirements, including the HKMA's banking regulatory requirements, applicable to banks:

1. TSP Information

2. TSP Governance and General Risk Management Policies and Procedures

3. Technology Risk Management and Cyber Security

4. Data Protection

5. Customer Care and Business Practices

6. Business Continuity Management

7. Outsourcing

Under the HKMA Open API Framework, in order to strike a balance between innovation and customer protection, it is preferred that TSPs offer solutions under a partnership arrangement with banks, and banks are therefore expected to adopt a formal TSP governance process.[5] The CB Requirements reflect considerations that are based on the legal and regulatory requirements that apply to banks. In order to address these compliance considerations during the TSP governance process, banks must consider the application of the CB Requirements to the TSPs with which they collaborate in the circumstances.

The CB Requirements are intended to represent a comprehensive set of business and risk management considerations that should apply to a bank's involvement in Phase II, III and IV API collaborations, unless otherwise indicated as being specifically relevant only to one or more Phases. Banks are bound by their relevant legal and regulatory requirements to *consider* all seven risk topics when assessing a collaboration but *may* decide that certain subtopics under the seven areas are *not* relevant to or required by the specific collaboration or in relation to the specific TSP.

Each area of assessment under the Common Baseline is adjusted by reference to the *nature* and *level* of risk involved in the specific collaboration, considering factors such as the nature of the bank's products and services to which the APIs relate, the sensitivity of the customer data being provided through the APIs, the risks involved in the transactions being instructed by the customer (in the case of Phase IV APIs) and the contemplated business arrangements between the parties.

---

4 Paragraph 40 of the HKMA Open API Framework.

5 Paragraph 29 of the HKMA Open API Framework.

There will be API collaborations where the risks to customers and the banking system are greater and so necessitate a more extensive evaluation of the TSP and the collaboration across the full range of CB Requirements risk management topics. On the other hand, a "lighter-touch", more streamlined application of the Common Baseline will be appropriate to simple API collaborations involving relatively low risk (in particular, the Simple Redirection Model of Phase II API collaborations). Please see the worked examples attached to the Common Baseline for illustration purposes.

As indicated, while the CB Requirements are intended to reflect a comprehensive set of business and risk management considerations, banks may choose to carry out additional checks that fit their needs but they should ensure that those checks are reasonable and not excessive.[6] Banks are expected to help TSPs understand how the CB Requirements could apply to the relevant proposed API collaboration in the event of doubt. For completeness, in addition to the TSP onboarding assessment and ongoing monitoring, banks are expected to negotiate bilateral commercial contracts with TSPs (including in relation to commercial aspects which are outside the scope of the CB Requirements).[7]

Application of the Common Baseline

Banks are required to assess TSPs and the proposed API collaboration before the launch of the services and on an on-going basis (as agreed in the bilateral agreement between the bank and the TSP). Assessments are to be fair, reasonable and commensurate with the risks involved and should include risk-based reviews of whether risk controls and risk management measures have been properly implemented in practice (in addition to TSPs providing undertakings to banks under legal agreements concerning the collaboration).

The Common Baseline has been drafted in principles-based, technology-neutral terms. Rather than using prescriptive language to describe specific technical or operational standards, such as a specific standard of encryption or a particular international standard, the Common Baseline has been prepared using words such as "reasonable" and "appropriate". This type of wording frames the CB requirements in flexible terms which are intended to make the application of the CB Requirements fair, reasonable and commensurate with the specific risks that arise in the context of a specific collaboration.

In general, the use, access or storage of customer data shared by the bank is only for the collaboration between the bank and TSP, as set out in the bilateral agreement. Separate explicit consent by the customer is required if the use, access or storage of customer data is extended to purposes other than the purposes of the collaboration. Adequate mitigating measures including, among others, those stated in Part 2 of Section 5 (Customer Care and Business Practices) are needed.

In order to aid in the understanding of how certain generic wording in the CB Requirements could apply specifically the Common Baseline will be updated from time to time to provide examples.

Phase III Open API Standards

It should be noted that a separate document, "The Phase III Open API Standards" was published by HKAB on 14 December 2021 (the "**Phase III Open API Standards**"). The Phase III Open API Standards serve a purpose different from that of the Common Baseline: they are intended to serve as a facilitation tool to support, and an example of the approach to the technical implementation of Phase III APIs, covering key areas of customer authentication, user experience, data handling, technical information security and operating standards.

---

6 Paragraph 38 of the HKMA Open API Framework.

7 Paragraphs 46 and 47 of the HKMA Open API Framework.

In assessing and applying the CB Requirements under the Common Baseline, banks may refer to standards identified or referred to in the Phase III Open API Standards.

Worked Examples for Phase II API collaborations

The Common Baseline requires that each API collaboration be assessed on the specific facts and circumstances of the collaboration. In order to aid in the interpretation and application of the Common Baseline, Appendix 2 (*Worked Examples*) incorporates the following worked examples for Phase II API collaborations:

Worked Example	Collaboration Type	Description
1	**Simple Redirection**	• The TSP provides a link redirecting the customer to the bank's production subscription/application interface. • No customer personal data is exchanged between the bank and the TSP. The customer is redirected by the link and makes a direct application for the bank's product or service on his or her own behalf. • The bank manages the application process directly with the customer.
2	**Lead Generation**	• The TSP provides basic contact details (name, email address and phone number) or other less sensitive customer information (such as reward scheme membership number and status) to the bank, enabling the bank to contact the customer directly. • After being contacted by the bank, the customer may then proceed to make a direct application for the bank's product or service on his or her own behalf. • The bank manages the application process directly with the customer. • Other than the contact details or other less sensitive customer information (such as reward scheme membership number and status) supplied by the TSP to the bank, no personal data is exchanged between the bank and the TSP.

Appendix 2 may be updated from time to time to provide illustrations where appropriate examples of Phase III or IV collaborations are received,.

Ongoing Compliance and Monitoring

In addition to carrying out the onboarding assessment to ensure fulfilment of the requirements of the Common Baseline and any additional requirements of the individual bank, the HKMA Open API Framework sets an expectation that banks will negotiate commercial agreements on a bilateral basis with TSPs, which, amongst others, should contain terms that are directed at ensuring ongoing compliance with these requirements, including:

1. define obligations on TSPs in relation to fulfilment of these requirements;
2. provide the bank with the ability to: (i) monitor the TSPs; and (ii) assess the TSP's relevant controls and their effectiveness in relation to fulfilment of these requirements;

3. provide for timely reporting and notification of significant incidents relating to the parties' collaboration; and
4. provide for the consequences of these requirements not being fulfilled.

Publication of List of Partnering TSPs

In order to promote public trust and consumer protection, each bank is expected to publish on its own website a list of TSPs with which it is partnering and the relevant products and services they will offer[8]. In addition, there is a central registry provided to the public with a list of partnering TSPs of banks and their relevant products. Banks should also provide updates to the list in a timely manner.

Ongoing Development of the Common Baseline

The Common Baseline is intended to be a "living document" that will likely change over time as banks and TSPs gain more experience with API collaborations and practical understandings of the CB Requirements develop.

The Common Baseline was first published on 15 November, 2019 to support the launch of Phase II of the HKMA Open API Framework.

The Common Baseline has been revised to introduce changes for the launch of Phases III and IV of the HKMA Open API Framework, with changes made to the CB Requirements specifically to address Phase III and IV API collaborations.

[8] Paragraph 48 of the HKMA Open API Framework.

Common Baseline

The requirements for onboarding TSPs should be fair and reasonable and commensurate with the risks involved.

The CB Requirements are intended to represent a comprehensive set of business and risk management considerations that should apply to a bank's involvement in Phase II, III and IV API collaborations, unless otherwise indicated as being specifically relevant only to one or more Phases. Banks are bound by their relevant legal and regulatory requirements to consider all seven risk management topics when assessing a collaboration but *may* decide that certain subtopics under the seven areas are *not* relevant to or required by the specific collaboration or in relation to the specific TSP.

Each area of assessment under the Common Baseline is adjusted by reference to the *nature* and *level* of risk involved in the specific collaboration, considering factors such as the nature of the bank's products and services to which the APIs relate, the sensitivity of the customer data being provided through the APIs and the risks involved in the transactions being instructed by the customer (in the case of Phase IV APIs) and the contemplated business arrangements between the parties.

1. TSP INFORMATION

CB Requirement	
1. The TSP has provided reasonably sufficient documentation and information (having regard to the nature and level of risk involved in the specific collaboration) to enable the bank to carry out reasonable due diligence as to the identity and reputation of the TSP, understand its business, its qualifications and experience and understand its operations and financial condition. Reference should be made to Appendix 1 – TSP Information in this regard, the bank requesting the categories of information described in Appendix 1 – TSP Information as appropriate in the context of the level of risk involved in the specific collaboration.	
2. The TSP has provided undertakings to the bank that are appropriate in the context with respect to:	
(a)	the truthfulness, accuracy and completeness of documentation and information provided by it to the bank as part of the bank's assessment of the TSP; and
(b)	the TSP's provision of updates of the documentation and information referred to in paragraph (a) in the event of any material change or inaccuracy.

2. TSP's Governance and General Risk Management Policies and Procedures

CB Requirement	
1. The TSP has provided reasonably sufficient documentation and information to demonstrate to the bank's reasonable satisfaction (having regard to the nature and level of risk involved in the specific collaboration) that:	
(a)	it has in place (i) policies and procedures for managing risk and (ii) internal control systems that are, in each case, appropriate and reasonably commensurate with the scale and complexity of the collaboration;
(b)	(i) in cases where the risks involved in the collaboration justify review at the individual level, the relevant managers and the officers, directors and controllers of the TSP are appropriately fit and proper having regard to their roles; (ii) the risk management functions within the TSP are sufficiently resourced and relevant personnel in these functions have sufficient professional knowledge, experience and independence to oversee the risk management and control functions of the TSP relating to the collaboration; and (iii) formal risk assessments are conducted periodically by relevant personnel with sufficient professional knowledge. The risk assessment should take into account objective analysis of any material change to the risk profile of the related services, emerging potential vulnerabilities and other risk related to the service. Where appropriate in light of the risks involved in the collaboration, the TSP's policy framework or related procedures for the formal risk assessment should require the risk assessment to be endorsed by designated senior officer(s) and be carried out at a frequency appropriate to the risk involved.

CB Requirement	
(c)	it has appropriate risk management functions to ensure compliance with: (i) the TSP's applicable legal and regulatory requirements as they relate to the collaboration; and (ii) the TSP's policies, procedures and controls, as each is relevant to the collaboration;
(d)	where appropriate in light of the risks involved in the collaboration, it has in place adequate policies, measures and procedures to manage reputational risks arising in its business; and
(e)	it has adequate record-keeping policies and systems for maintaining accurate and sufficient records as reasonably necessary to the collaboration.
2. The TSP has provided undertakings to the bank that are appropriate in the context with respect to:	
(a)	the TSP's compliance with its relevant risk management policies and procedures;
(b)	the TSP's performance of its obligations in respect of the collaboration in a manner that enables the bank to meet its relevant regulatory requirements from time to time;
(c)	the TSP's provision of: (i) reports and information; and (ii) access to relevant information, personnel and records, in each case, as reasonably necessary for the bank to undertake reasonable monitoring of risks relating to the collaboration, including in respect of any collaboration in which the TSP functions as an intermediary in respect of the bank's products and services; and
(d)	the TSP's continued responsibility for operations that have been sub-contracted or outsourced by the TSP to any third party.

3. Technology Risk Management and Cyber Security

	CB Requirement
1. The TSP has provided reasonably sufficient documentation and information to demonstrate to the bank's reasonable satisfaction (having regard to the nature and level of risk involved in the specific collaboration) that it has in place technology risk management policies and procedures that are reasonably commensurate with the scale and complexity of the TSP business relevant to the API collaboration.	
2. Without limiting the generality of paragraph 1, the TSP has provided reasonably sufficient documentation and information to demonstrate to the bank's reasonable satisfaction (having regard to the nature and level of risk involved in the specific collaboration) that its technology risk management framework relevant to the collaboration:	
(a)	is appropriate for ensuring: (i) adequate IT controls, (ii) the quality and security, including the reliability, robustness, stability and availability, of its systems, (iii) the safety and efficiency of its operations, and (iv) adequate control over sub-contractors, in each case, as relevant to the collaboration;
(b)	includes appropriate testing of systems, networks and applications (including, each to the extent appropriate having regard to the risks of the specific collaboration: (i) code reviews and penetration testing; (ii) security testing such as vulnerability testing (including, as appropriate, through independent assessment and testing)) prior to launch, prior to the deployment of any major release, upgrade or other material change (and in any event no less frequently than once per year);
(c)	includes appropriate configuration hardening on: (i) Internet facing aspects of its applications, systems and networks; and (ii) (where highly sensitive customer information is involved) internal applications, systems and networks;
(d)	includes appropriate encryption measures to protect the confidentiality of customer information transmitted through the APIs as part of the collaboration, and where sensitive customer information is involved, encryption and transmission over internal networks and storage;

(e)	includes appropriate measures to ensure the availability of systems relevant to the collaboration, including: (a) appropriate capacity planning and performance monitoring; and (b) appropriate access control configurations and measures to monitor and limit API usage in accordance with any applicable API fair usage policies;
(f)	includes appropriate change management procedures in respect of its applications, systems and networks in production;
(g)	includes appropriate monitoring systems and techniques in relation to fraud and system security, involves appropriate vulnerability assessments in relation to security threats and appropriate security patch workflows;
(h)	includes an incident management and response framework with sufficient management oversight to ensure effective incident response and management capability to identify significant incidents, establish their root cause, make necessary notifications to stakeholders and deal with the incident properly so as to ensure risks and customer impacts are managed and minimised;
(i)	includes, to the extent appropriate, training and professional accreditation for personnel engaged in roles responsible for ensuring operational cyber resilience;
(j)	includes appropriate and effective security controls for personnel that have access to sensitive customer data, including maintaining and reviewing audit logs and investigating, escalating and reporting incidents of potential misuse;
(k)	includes, to the extent appropriate, having regard to the risks involved in the collaboration, adequate measures to maintain appropriate segregation of databases for different purposes to prevent unauthorized or unintended access or retrieval and that robust access controls are enforced to ensure the confidentiality and integrity of the databases;
(l)	includes (as necessary and as appropriate) procedures and measures for monitoring trends in cyber threats, implementing adequate protective measures and performing periodic security testing; and
(m)	includes, in respect of Phase III API collaborations, appropriate integrations, endpoints, encryption controls, input validation controls, permissions and other requirements in relation to customer authentication[9] and processes for customers to grant and revoke consent to the TSP's access to their data.
3. Without limiting the generality of paragraph 1, the TSP has made adequate disclosure of information and documentation supporting the assessment by the bank of the matters referred to in paragraph 2, including details of: (i) any known vulnerabilities in its applications, systems or networks; (ii) any data breach or information security incident in the previous 2 years relating to the TSP's relevant applications and systems (including satisfactory explanation of how these matters were resolved and the preventative measures taken to reduce the risk of recurrence); (iii) any use of "end of life" or unsupported software in its systems and how this use is effectively managed; and (iv) (as necessary and appropriate) the TSP's procedures to detect fraudulent or unauthorized access to the APIs.	
4. The TSP has provided undertakings to the bank that are appropriate in the context with respect to:	
(a)	the application of industry practices to the development, testing and operation of relevant applications, systems and networks and compliance with its internal policies and procedures in respect of technology risk management;
(b)	compliance with specific technology risk management requirements agreed by the bank and the TSP, as being appropriate to the circumstances of the collaboration, including with respect to technology risk areas such as customer authentication of access to APIs (having regard to the nature and level of risks of transaction(s) to be undertaken), customer consent management and compliance with any agreed API fair usage policies;
(c)	the TSP's performance of its obligations in respect of the collaboration in a manner that enables the bank to meet its relevant regulatory requirements from time to time;

[9] It would be prudent for TSPs to avoid collecting or storing customers' e-banking login credentials on the TSPs' own platforms.

(d)	providing the bank with contact details of appropriate personnel responsible for information security within the TSP's organization;
(e)	notifying the bank on appropriate agreed timescales of any disruption or unauthorized access to applications, systems and/or networks relating to the collaboration, and regular monitoring of fraudulent website and apps by TSP;
(f)	carrying out appropriate monitoring, identification, assessment and mitigation of fraudulent activities in relation to the usage of and access to APIs;
(g)	in relation to Phase III API collaborations: i. provide customers with a process to revoke their consent to sharing their data with the TSP; ii. informing the customer of the consequences of their revocation of consent to share their data with the TSP before the TSP takes such action; and iii. notifying the bank in the event of the active removal of a customer account by the TSP; and
(h)	performing, within appropriate timescales, remediation work necessary to address any failure of the TSP's applications, systems or networks to meet any of the requirements of this part.

4. Data Protection

	CB Requirement
1. The TSP has provided reasonably sufficient documentation and information to demonstrate to the bank's reasonable satisfaction (having regard to the nature and level of risk involved in the specific collaboration) that:	
(a)	it will collect personal data from customers in relation to the collaboration in a fair and transparent manner that complies with the Personal Data (Privacy) Ordinance ("**PDPO**") and any applicable codes of practice;
(b)	it has in place adequate policies, measures and procedures to protect customers' information from unauthorized access, unauthorized retrieval, tampering and misuse, including appropriate restrictions on its personnel's access to personal data; and
(c)	in respect of Phase III API collaborations, it has in place adequate policies, measures and procedures to manage the customer onboarding journey (in respect of the obtaining, refreshing and withdrawal of consents).
2. The TSP has provided undertakings to the bank that are reasonably sufficient in the context to:	
(a)	ensure that the TSP complies with its relevant data protection policies and procedures, including with respect to the following (in each case, in respect of the collaboration): (i) maintaining and managing data subject notifications and consents (including complying with withdrawals of consents); (ii) data subject access and correction requests; (iii) protecting customers' information from unauthorized access, unauthorized retrieval, tampering; and (iv) misuse and ensuring the accuracy of any customer information provided to the bank;
(b)	ensure that the TSP's performance of its obligations in respect of the collaboration in a manner that enables the bank to meet its relevant data protection regulatory requirements from time to time;
(c)	comply with the requirements of the PDPO and any applicable codes of practice in respect of the collection, use, holding, processing and erasure of personal data in connection with the collaboration, including by: (i) making necessary (and appropriately prominent) notifications to and obtaining, maintaining and allowing for the withdrawal of necessary (and appropriately explicit) consents from customers in respect of: (A) transfers of personal data between the bank and the TSP in relation to the collaboration; and

	CB Requirement
	(B) the retention of personal data by the TSP for use, access, storage and processing for the TSP's own business purposes separate from the collaboration, and not make any misrepresentations with respect to such collection, processing and transfers; and (ii) complying with the requirements of PDPO in respect of data minimisation;
(d)	notify in a timely manner the bank of any loss or unauthorized access to or misuse of customer data relating to the collaboration; and
(e)	comply with any specific requirements agreed by the bank and the TSP in respect of data usage and data sharing, including obligations to process data in accordance with the purposes for which the data has been collected, such requirements being consistent with considerations under this CB Requirement and the risks of the specific collaboration.

5. Customer Care and Business Practices

	CB Requirement
1. The TSP has provided reasonably sufficient documentation and information to demonstrate to the bank's reasonable satisfaction (having regard to the nature and level of risk involved in the specific collaboration) that:	
(a)	it has appropriate policies and procedures in place in its relevant business directed at ensuring the TSP acts in a responsible, honest and professional manner, treats customers equitably, honestly and fairly with regard to matters such as clearly explaining the key features, risks and terms, value proposition to the consumer of financial services products, and providing accurate and understandable information;
(b)	there are appropriate means of ensuring that any information relating to the bank's products and services which are provided to customers by the TSP are accurate, honest and understandable and not misleading;
(c)	it has appropriate policies, procedures and measures in place to detect and prevent fraud against customers in relation to the collaboration and the collaborated services, including policies, procedures and measures relating to: (i) customer authentication and consent management; and (ii) secure access to APIs; and
(d)	it has in place an effective and fair complaint and redress management system for customers to make complaints and seek redress and for the bank to address and handle complaints/redress in relation to the collaboration and the collaborated services.
2. The TSP has provided undertakings to the bank that are appropriate in the context with respect to:	
(a)	requiring the TSP to deal with customers in accordance with applicable laws and regulations and in accordance with good industry practice and notify the bank of customer complaints relating to the collaboration;
(b)	the TSP's performance of its obligations in respect of the collaboration in a manner that enables the bank to meet its relevant regulatory requirements issued from time to time;
(c)	requiring the TSP to: (i) prominently display a standard message specified by the bank (including a link to the bank's webpage) in the TSP's user interface in order to distinguish which services are provided in collaboration with the bank and which services are not; and (ii) in relation to Phase II API collaborations, where customers' contact details are collected by and passing through the TSP to the bank for the latter to further approach the customer, prominently display an educational message at the TSP's user interface upon such collection communicating to customers that:

	(1) customers should first authenticate the identity of the callers or senders who purport to be the bank's representatives, using the relevant bank's hotlines for this purpose, which can be found at the bank's official website or the HKMA's website, and (2) the most prudent way for customers to continue the application process after authentication is to contact the bank's representative using the phone number obtained from the bank's authentication hotline.
(d)	carrying out appropriate monitoring for fraudulent websites, apps, emails or other fraud schemes related to the TSP and promptly notifying the bank and the public of such schemes where relevant;
(e)	without limiting paragraph (b) above, providing proper disclosure and adequate transparency to customers in relation to the collaboration in a manner that meets the bank's obligations, ensuring the TSP's customer journey design enables informed decision-making by customers and does not misrepresent the bank's products or services;
(f)	ensuring the TSP's interfaces, as they relate to the collaboration meet the needs of customers with disabilities; and
(g)	as appropriate, requiring the TSP to maintain insurance coverage appropriate to the risks involved in the collaboration (as specifically agreed between the bank and TSP).
3. The Bank and the TSP should agree and document clear principles of liability and settlement, customer complaint and redress management arrangements for compensating customers' losses arising from customer complaints, unauthorized transactions and other disputes in relation to the collaboration, with clear communication to customers at the outset. The Bank and the TSP should agree terms and conditions addressing issues such as: (i) the circumstances in which either party will be liable for unauthorized transactions; (ii) the mechanism for resolving disputes in relation to the parties' liability; and (iii) the arrangements for paying compensation to the customer pending resolution of any dispute. The arrangement should adhere to the principle that a customer should not be responsible for any direct loss suffered by him/her as a result of unauthorized transactions conducted through his/her account attributable to the products or services unless the customer acts fraudulently or with gross negligence.	

6. Business Continuity Management

	CB Requirement
1. The TSP has provided reasonably sufficient documentation and information to demonstrate to the bank's reasonable satisfaction (having regard to the nature and level of risk involved in the specific collaboration) that:	
(a)	it has in place adequate business continuity management programs directed at ensuring continuation, timely recovery, or in extreme situations, orderly scale-down of critical operations in the event of major disruptions caused by different contingent scenarios; and
(b)	it has in place an appropriate business exit plan that seeks to provide for an orderly exit of its business as it relates to the collaboration and minimize the impact on its customers.
2. The TSP has provided undertakings to the bank that are reasonably sufficient in the context to comply with the TSP's business continuity and disaster recovery arrangements and any specific business continuity and disaster recovery arrangements agreed by the parties as appropriate in the circumstances of the collaboration.	

7. Outsourcing

CB Requirement
To the extent that the collaboration with the TSP involves any outsourcing by the TSP (including any outsourcing to its affiliates), the TSP must ensure its continued compliance with its obligations under its bilateral agreement with the bank, that it retains sufficient control over the relevant operations and has

CB Requirement
undertaken appropriate risk management in relation to the selection of the third party and the implementation and monitoring of the sub-contracting or outsourcing arrangement. Areas of controls should include but not limited to the following: - data protection; and - assurance of the management of technology risk and cyber security.

Appendix 1 – TSP Information

1. General Information about the TSP

	Question/ Requirement
(a)	Name of the TSP
(b)	Trading name(s) other than as provided in a), if applicable
(c)	Type of entity (please tick): • sole proprietor • general partnership • limited partnership • private limited company • public limited company • company limited by guarantee • other.
(d)	Please provide Hong Kong Business Registration details and certificate
(e)	Listing information, if any
(f)	Jurisdiction of establishment/incorporation
(g)	If the TSP is a foreign company, please provide details of its Foreign Company Registration in Hong Kong
(h)	For TSPs who are companies or limited partnerships, please provide: • registration number • head office address • registered office address (if different) Please attach certificate of registration/incorporation and articles of association
(i)	Please complete and submit a **TSP Individual Form** (Annex 1) in respect of each director and senior manager of the applicant, or, as directed by the bank, provide an internal corporate governance structure chart illustrating management roles and reporting lines.
(j)	Please complete and submit a **TSP Controller Form** (Annex 2) in respect of each person or entity holding (directly or indirectly) an interest in the applicant of 10% or more or exercising control of the TSP by other means

2. Business Description

	Question/ Requirement
(a)	Please provide a description of the TSP's current business model, including the products and services it currently makes available and any services that it will offer to customers in connection with use of the APIs
(b)	Please provide a description of the specific APIs the TSP intends to use and how it intends to use these APIs in its business

	Question/ Requirement
(c)	Please provide details of any regulatory licenses held by the TSP or regulated services provided
(d)	Please provide website address(es) used by the TSP's business

3. Operational Description

	Question/ Requirement
(a)	Please provide a copy of the TSP's organisational chart, showing key divisions, departments, structural separation of the TSP
(b)	Please provide a description of key individuals and members of the TSP's staff and their respective experience and qualifications for roles as specified by the bank
(c)	Please provide details of any material arrangements the TSP has with third parties relating to the use of the specific APIs that it intends to use, such as: • collaborations with third parties enabling the TSP to gain access to or attract prospective customers; • outsourcing arrangements; and/or • key operational dependencies on third parties, such as technology providers, information or data providers, data processing service providers or other service providers.
(d)	Please provide a description of the workflows and information flows the TSP expects to have in place in relation to the specific APIs it intends to use in its business, including the following: • the context of the APIs and how the user experience directs the customer to the APIs; • the sources of data the TSP will submit to the bank through the APIs (whether inputted by the customer, taken from existing data held by the TSP or obtained from third party sources); • what personal data the TSP will collect from customers as part of this workflow and how the TSP proposes to use this personal data; and • what, if any, data the TSP will need to receive from the bank as part of these arrangements (for example, application status) • any internal information firewall/barrier ring-fencing the APIs to the teams on a necessity, need-to-know basis for the proposed use of the APIs

4. Business Overview and Financials

	Question/ Requirement
(a)	Please provide the TSP's business overview, including the following information: • general description of the market in which the TSP operates; • summary proposal of how the TSP intends to use and present the API (and the related bank products and services) as part of its business activity; • general description of the TSP's customer groups; • certified accounts for the past two financial years or a description of the TSP's financial situation if not available; and • appropriate evidence of financial soundness.
(b)	Please provide details of the TSP's insurance cover.

Annex 1 - TSP Individual Information Form

	Question/ Requirement
(a)	Name of the TSP
(b)	Name of the TSP Individual (including: (1) surname; and (2) first and middle names)
(c)	Title
(d)	Any previous or other names used (and dates of name changes in the case of previous names)
(e)	Gender
(f)	Date and place of birth
(g)	Nationality
(h)	Hong Kong Identification Card number or copy of passport/travel document
(i)	Current and previous addresses (together with dates) for previous **[*]** years
(j)	Position/role in the applicant and relevant date of commencement for each position/role
(k)	Description of responsibilities with the applicant
(l)	Employment history for past **[*]** years, including employer, employer address, period of employment, position held, responsibilities and reasons for leaving for each
(m)	Details of any criminal convictions or proceedings in the past **[*]** years
(n)	Details of any personal bankruptcy or analogous proceedings in any jurisdiction in the past **[*]** years
(o)	Details of any civil or administrative proceedings against the individual in the past **[*]** years

Annex 2 – TSP Controller Information Form

	Question/ Requirement
(a)	Name of the TSP
(b)	Name of the TSP Controller
(c)	Percentage interest held by the TSP Controller (directly or indirectly) in the TSP
(d)	Please complete and submit a TSP Individual Form if the TSP Controller is an individual/natural person
(e)	If the TSP Controller is a legal entity, please complete (f) to (q)
(f)	Trading name(s) other than as provided in (b), if applicable
(g)	Type of entity (please tick): • sole proprietor • general partnership • limited partnership • private limited company • public limited company • company limited by guarantee • other
(h)	Please provide Hong Kong Business Registration details and certificate
(i)	Listing information, if any
(j)	Jurisdiction of establishment/incorporation
(k)	If the TSP Controller is a foreign company, please provide details of foreign company registration in Hong Kong
(l)	For companies and limited partnerships, please provide: • registration number • head office address • registered office address (if different) Please attach certificate of registration/incorporation and articles of association
(m)	Please describe principal business activities of the TSP Controller
(n)	Please describe regulatory authority and licensing requirements, if any, applicable to the TSP Controller
(o)	Details of any criminal convictions or proceedings in the past [*] years
(p)	Details of any bankruptcy, insolvency or analogous proceedings in any jurisdiction in the past [*] years
(q)	Details of any civil or administrative proceedings against the TSP Controller in the past [*] years

Appendix 2 – Worked Examples

1. Worked Example for Simple Redirection API Collaboration

Description of Typical API Collaboration

In a typical case, a Simple Redirection collaboration will involve the TSP providing customers with a link which they may use to access the bank's product or service subscription site. The TSP does not provide the bank with any of the customer's personal data or initiate an application for the bank's products or services on behalf of the customer. Once the customer has been redirected to the bank's product or service subscription site, the customer may choose to initiate an application on their own behalf. The bank manages the application process directly with the customer.

Worked Example

There may be risk factors distinguishing specific Simple Redirection Collaborations from each other, but the following represents a typical application of the Common Baseline to a Simple Redirection Collaboration:

No.	Common Baseline Topic	Specific Requirements
1	TSP Information	• TSP must complete sections 1 (a) – (h) (General Information about the TSP) as specified in Appendix 1 (TSP Information). Note that the TSP Individual Information Form and TSP Controller Information Forms set out in Annexes 1 and 2 to Appendix 1 are not expected to apply. • TSP may be required to provide additional information and documentation about TSP and/or information about TSP Controllers as required by applicable law. • Bank's agreement with the TSP must include the undertakings set out in section 2.
2	TSP's Governance and General Risk Management Policies and Procedures	• Bank's agreement with the TSP must include the undertakings set out in sections 2 (b) – (d).
3	Technology Risk Management and Cyber Security	• TSP must provide information to the bank regarding its monitoring in relation to system security of its relevant site as per section 2(g), in particular how TSP will ensure that customers are not misled or misdirected to sites other than the bank's relevant site. • Bank's agreement with the TSP must include the undertakings set out in sections 4 (a) – (e) and (h).
4	Data Protection	• Not applicable.
5	Customer Care and Business Practices	• TSP must provide the bank with information concerning how it will promote the bank's products and services in connection with the redirection link, as per sections 1(b) and (c).

No.	Common Baseline Topic	Specific Requirements
		• TSP must provide the bank with information concerning its complaint management system, as is relevant to the redirection link, as per section 1(d). • Bank's agreement with the TSP must include the undertakings set out in sections 2 (a) to (f) and section 3.
6	Business Continuity Management	• Not applicable.
7	Outsourcing	• TSP must provide details of any outsourcing of the operation of the link directing traffic to the bank's site (and other relevant aspects of the TSP's site) and how TSP will ensure compliance with the terms and conditions of its agreement with the bank in the case of any such outsourcing.

Please note that each specific API collaboration must be judged on the basis of the specific risks involved. The worked example set out above may not apply in any specific case. Additional requirements may apply.

2. WORKED EXAMPLE FOR LEAD GENERATION API COLLABORATION

Description of Typical API Collaboration

In a typical case, a Lead Generation API collaboration will involve the TSP collecting contact details from the customer (name, email address and phone number) and other less sensitive customer information (such as reward scheme membership number and status) and, with the customer's consent, providing these details to the bank so that the bank may initiate communications with the customer promoting the bank's products and services.

The TSP does not provide the bank with any customer information other than the contact details and other less sensitive customer information (such as reward scheme membership number and status). Once contacted through the bank's marketing communications, the customer may choose to initiate an application with the bank himself/herself. The bank manages the application process directly with the customer.

Worked Example

There may be risk factors distinguishing specific Lead Generation API Collaborations from each other, but the following represents a typical application of the Common Baseline to a Lead Generation API Collaboration:

No.	Common Baseline Topic	Specific Requirements
1	TSP Information	• TSP must complete sections 1 (a) – (h) (General Information about the TSP) as specified in Appendix 1 (TSP Information). Note that the TSP Individual Information Form and TSP Controller Information Forms set out in Annexes 1 and 2 to Appendix 1 are not expected to apply. • TSP may be required to provide additional information and documentation about TSP and/or information about TSP Controllers as required by applicable law. • Bank's agreement with the TSP must include the undertakings set out in section 2.
2	TSP's Governance and General Risk Management Policies and Procedures	• Bank's agreement with the TSP must include the undertakings set out in sections 2 (b) – (d).
3	Technology Risk Management and Cyber Security	• TSP must provide information to the bank regarding the security and monitoring of the systems and networks involved in the collection, processing and storage of the customer data and the transmission of this data to the bank as per section 2(g). • Bank's agreement with the TSP must include the undertakings set out in sections 4 (a) – (e) and (h).
4	Data Protection	• As per section 1(a), TSP must provide copies of its personal information collection statements and other policies relating to the collection of customer personal data and be expected to provide the bank with information

No.	Common Baseline Topic	Specific Requirements
		reasonably demonstrating the TSP's compliance with such policies and otherwise demonstrating that: o the collection of personal data from customers was carried out fairly, transparently and otherwise in accordance with the requirements of the PDPO; o the personal data provided to the bank is accurate and the TSP will take steps to correct any data once it learns that it is inaccurate; o the personal data will be processed securely in accordance with the requirements of the PDPO and will only be used for the purposes for which the data has been lawfully collected; and o the customers have consented to the transfer of their personal data to the bank for the bank's marketing purposes in accordance with the requirements of the PDPO. o Also as per section 1(b), the TSP is expected to provide the bank with information reasonably demonstrating that the TSP has adequate systems and procedures in place to receive and record customers' choices to opt-out of receiving direct marketing and promptly communicate these opt-outs to the bank. • Bank's agreement with the TSP must include the undertakings set out in sections 2 (a) – (e).
5	Customer Care and Business Practices	• TSP must provide the bank with information concerning how it will promote the bank's products and services in connection with the collection of customer personal data, as per sections 1(b) and (c). • TSP must provide the bank with information concerning its complaint management system, as is relevant to the collection of customer contact details as per section 1(e). • Bank's agreement with the TSP must include the undertakings set out in sections 2 (a) – (f) and section 3. • Where customers' personal data are collected by and transferred by the TSP to the bank for the latter to further approach the customers, the TSP must clearly explain these arrangements in the screen flow and display a prominent educational message communicating that: o customers should first authenticate the identity of those who purport to be the bank's representatives using the relevant bank's contact details for this purpose, which contact details can be found at the bank's official website or the HKMA's website; and o the most prudent way for customers to continue the application process after

No.	Common Baseline Topic	Specific Requirements
		authentication is to contact the bank's representative using the phone number obtained from the bank's authentication hotline.
6	Business Continuity Management	• Not applicable.
7	Outsourcing	• TSP must provide details of any outsourcing of the operation of the collection, processing and/or storage of customer contact details (and other relevant aspects of the TSP's site) and how TSP will ensure compliance with the terms and conditions of its agreement with the bank in the case of any such outsourcing.

Please note that each specific API collaboration must be judged on the basis of the specific risks involved. The worked example set out above may not apply in any specific case. Additional requirements may apply.