OPEN BANKING MODULE

MODULE:	OB (Open Banking)

Table of Contents

OB-A.1 Purpose

OB-A.1.1 This Module sets out the Central Bank of Bahrain's (CBB's) Directive relevant to ancillary service providers providing either or both of the following regulated services defined in the Ancillary Services Authorisation Module of the CBB Rulebook Volume 5 in the Kingdom of Bahrain:

(a) the provision of account information services; or
(b) the provision of payment initiation services.

OB-A.1.2 This Module should be read in conjunction with the requirements in other parts of the CBB Rulebook, Volume 5, applicable to specialised licensees particularly:

(c) Ancillary Service Providers Authorisation Module;
(d) Principles of Business Module;
(e) General Requirements Module;
(f) CBB Reporting Requirements Module
(g) Auditors and Accounting Standards Module;
(h) Financial Crime Module; and
(i) Enforcement Module.

Legal Basis

OB-A.1.3 **This Module contains the CBB's Directive (as amended from time to time) applicable to ancillary services providers undertaking account information services or payment initiation services, and is issued under the powers available to the CBB under Article 38 of the CBB Law.**

OB-A.1.4 For an explanation of the CBB's rule-making powers and different regulatory instruments, see Section UG-1.1.

OB-A.2 Module History

OB-A.2.1 This Module was first issued in November 2018. It is numbered as version 01. All subsequent changes to this Module are annotated with a sequential version number. UG-3 provides further details on Rulebook maintenance and version control.

OB-A.2.2 A list of recent changes made to this Module is provided below:

Module Ref.	Change Date	Description of Changes

MODULE	OB:	Open Banking
CHAPTER	OB-B:	Scope of Application

OB-B.1 Introduction

OB-B.1.1 The provision of account information services and payment initiation services entails obtaining access to customer accounts through 'application program interfaces' (APIs) with licensees maintaining customer accounts include conventional retail bank licensees, Islamic retail bank licensees financing companies and PSPs operating electronic wallets, (referred to in this Module as "licensees maintaining customer accounts"). Given the nature of risks inherent in online activities, the ancillary service providers undertaking such activities will be subject to strict regulatory standards to ensure the integrity and safety of customer data, the APIs, customer on boarding process, authentication process, communication sessions, process for tracking of security incidents and associated standards of dealing with the customers while undertaking this activity.

OB-1.1 Risks, Systems and Controls

Internal Controls

OB-1.1.1 The Board of Directors or equivalent authority must take responsibility for the establishment and oversight of effective risk management and internal controls.

OB-1.1.2 Account information service providers (AISPs) and payment initiation service providers (PISPs) must use technology solutions which are capable of interfacing with software and systems used by licensees maintaining customer accounts with no material modifications to their systems.

OB-1.1.3 Consistent with Module PB: Principles of Business, Paragraph, PB-1.1.10, AISPs and PISPs must establish adequate internal controls to safeguard the business, its customers and licensees to which they have online access to.

OB-1.1.4 The internal controls must include, but not be limited to, those relating to the following:

(a) The development and or acquisition of the technology solutions to conduct the activity;
(b) Testing of the solutions and application program interfaces;
(c) Standards of communication and access and security of communication sessions;
(d) Safe authentication of the users;
(e) Processes and measures that protect customer data confidentiality and personalised security credentials consistent with Law No. 30 of 2018, Personal Data Protection Law (PDPL) issued on 12 July 2018;
(f) Tools and measures to prevent frauds and errors;
(g) Security policy;
(h) Information security testing including web applications testing, configuration reviews, penetration testing and smart device application testing
(i) Risk management controls;
(j) Prevention of anti-money laundering (AML) and combating terrorist financing (CTF);
(k) Record keeping and audit trails; and
(l) Operational and financial controls.

OB-1.1 Risks, Systems and controls (continued)

Operational Risks

OB-1.1.5 **AISPs and PISPs must document the process by which they identify, prioritise and manage their operational risks.**

OB-1.1.6 Operational risk in AISPs' and PISPs' activities include the risk of loss of confidential customer data, financial loss or reputational loss resulting from inadequate or failed internal processes, people, technology and systems, or from external events including risks of internal and external frauds and cyber threats. In assessing potential operational risk, the following are some of the factors that may affect the licensee's risk exposure:

(a) Lack of governance, board and management oversight;
(b) Inadequate internal controls;
(c) Insufficient transaction monitoring;
(d) Failure of information technology through breakdown, incompatibility of legacy systems and poor scalability, poor security, etc.;
(e) Failure or insufficient cyber and information security controls;
(f) Failure of processes and procedures;
(g) Internal and external fraud;
(h) Legal risks;
(i) Outsourcing risk;
(j) Business continuity and disaster recovery; and
(k) Reputational risks.

OB-1.1.7 **AISPs and PISPs must establish comprehensive procedures for monitoring, handling and following up on security and fraud incidents and related customer complaints including but not limited to the following:**

a) organisational measures and tools for the prevention of such incidents;
b) details of the individual(s) and bodies responsible for assisting customers in cases of the incidents and technical issues and/or claim management;
c) reporting lines in cases of such incidents;
d) the contact point for customers, including a name and email address;
e) the procedures for the reporting of incidents, including the communication of these reports to internal or external bodies, including notification of major incidents to national competent authorities; and
f) the monitoring tools used and the follow-up measures and procedures in place to mitigate security and fraud risks.

OB-1.1 Risks, Systems and controls (continued)

OB-1.1.8 AISPs and PISPs must maintain an up to date security policy document containing the following information:

a) A detailed documentation of the technology architecture and of the systems and the network elements providing:
   i. a description of the business IT systems supporting the business activities;
   ii. the type of authorised connections from outside, such as with partners, service providers, entities of the group and employees working remotely, including the rationale for such connections;
   iii. for each of the connections, the logical security measures and mechanisms in place, specifying the control the licensee will have over such access as well as the nature and frequency of each control,
   iv. process for the opening/closing of communication lines, and description of security equipment configuration, generation of keys or client authentication certificates, system monitoring, authentication, confidentiality of communication, intrusion detection, antivirus systems and logs;
b) the logical security measures and mechanisms that govern the internal access to IT systems;
c) the physical security measures and mechanisms of the premises and the data centre of the licensee, such as access controls and environmental security;
d) the security of the account information and payment initiation processes, which should include:
   i. the customer authentication procedures used for both consultative and transactional access, and for all underlying payment instruments;
   ii. an explanation of how safe delivery of tokens to the legitimate customer; and
   iii. a description of the integrity of authentication factors, tokens and online and mobile applications at the time of both initial enrolment and renewal.

OB-1.1 Risks, Systems and controls (continued)

OB-1.1.9 AISPs and PISPs must ensure they have an up to date business continuity plan and arrangements consisting of the following information:

a) a business impact analysis, including the business processes and recovery objectives, such as recovery time objectives, recovery point objectives and protected assets;
b) the identification of the back-up site, access to IT infrastructure, and the key software and data to recover from a disaster or disruption;
c) an explanation of how the licensee will deal with significant continuity events and disruptions, such as the failure of key systems; the loss of key data; the inaccessibility of the premises; and the loss of key persons; and
d) the frequency with which the licensee intends to test the business continuity and disaster recovery plans, including how the results of the testing will be recorded.

OB-1.1.10 AISPs and PISPs must appoint a third party specialist to conduct vulnerability assessments against cyber-attacks and penetration testing on the specific API security standards every 6 months. The specialist's report must be submitted to the CBB, along with the licensee's related action plan to resolve any issues identified. All relevant threat profiles referenced in the security standards including the risk of social engineering must be considered for the reviews.

OB-1.1.11 AISPs and PISPs must ensure that their overall systems and controls including but not limited to the business continuity, disaster recovery, information security testing, web-applications testing, smart device application testing, and cyber resilience are evaluated and independently tested by an external consultant:

a) initially upon implementation of this Module;
b) when there are any material changes to the systems and controls; and
c) at least once every 3 years.

OB-1.1 Risks, Systems and controls (continued)

OB-1.1.12 A PISP must establish payment initiation procedures to ensure:

(a) that a customer's personalised security credentials are:
   i. not accessible to other parties, with the exception of the issuer of the credentials; and
   ii. transmitted through safe and efficient channels;

(b) that any other information about a customer is not provided to any person except a payee, and is provided to the payee only with the customer's explicit consent;

(c) that each time a customer initiates a payment order, identify himself to the PISP, the licensee with who he maintains the account in a secure way;

(d) that it will not store sensitive data (such as customer security credentials or other personalized data, the holding of which is not authorized by the customer, and data which may be used by the holder for unauthorized, fraudulent or illegal activity or transactions) of the customer;

(e) that it will not use or access any information for any purpose except for the provision of a payment initiation service explicitly requested by a payer;

(f) that it cannot and does not change the amount, the payee or any other feature of a transaction notified to it by the customer.

OB-1.1.13 An AISP must establish account information procedures to ensure:

(a) it does not provide account information services without the customer's explicit consent;

(b) that the customer's personalised security credentials are:
   i. not accessible to other parties, with the exception of the issuer of the credentials; and
   ii. transmitted through safe and efficient channels;

(c) for each communication session, communicate securely with licensee and the customer in accordance with the regulatory requirements of this Module;

(d) that it does not access any information other than information from designated accounts; and

(e) it cannot and does not use, access or store any information for any purpose except for the provision of the account information service explicitly requested by the customer.

OB-2.1 Framework Contracts

Legal arrangement and transparency

OB-2.1.1 AISPs and PISPs must establish a framework contract (a legal arrangement) with the customer. They must also provide the customer the information set forth below prior to being bound by the framework contract for the services to be provided:

(a) The following information about the service and the provider:

i. the name, address and contact details of the PISP or AISP as the case may be;

ii. a description of the main characteristics of the service to be provided;

iii. the information or unique identifier that must be provided by the customer in order for a payment order to be properly initiated or executed;

(b) the form and procedures for giving consent to provide account information service, the initiation of a payment order and for the withdrawal of consent;

(c) provisions regarding the time of receipt of a payment order and the cut-off time, if any, established by the licensee and the maximum execution time for the payment services to be provided;

(d) whether spending limits for the use of a payment instrument may be agreed;

(e) the detail of all fees and charges payable by the customer to the PISP/AISP, including those connected to the manner in and frequency with which information is provided or made available and, where applicable, a breakdown of the amounts of any charges;

(f) the means of communication agreed between the parties for the transmission of information or notifications under this Module including, where relevant, any technical requirements for the customer's equipment and software for receipt of the information or notifications;

(g) The terms under which the customer may opt out from the use of the payment instrument;

(h) explicit consents required for generic marketing promotions by the PISP/AISP; and

(i) the terms of the framework contract and information.

OB-2.1 Framework Contracts (continued)

(j) The following information about safeguards and corrective measures:

i. where relevant, a description of the steps that the customer is to take in order to keep safe a payment instrument and how to notify the PISP/AISP for the purposes of obligations of the customer in relation to loss, theft, misappropriation, unauthorised use of the payment instruments and personalised security credentials;

ii. the secure procedures, by which the PISP/AISP will contact the customer in the event of suspected or actual fraud or security threats;

iii. the conditions under which the PISP/AISP stops or prevents the use of a payment instrument;

iv. the customer's liability, (payer or payee's liability for unauthorized payment transactions), including details of any limits on such liability;

v. how and within what period of time the customer is to notify the licensee maintaining customer account of any unauthorised or incorrectly initiated or executed payment transaction, and liability, if any for unauthorised payment transactions falling on the licensee maintaining customer account for execution of unauthorised payment transactions);

vi. liability, if any, in the event of initiation or execution or non-execution or defective or late execution of payment transactions;

vii. liability of parties in the event of a cyber-attack and loss of sensitive data; and

viii. the conditions for any refunds for payment transactions initiated by or through a payee.

OB-2.1 Framework Contracts (continued)

(k) The following information about changes to and termination of the framework contract:

i. the time given to the customer to review and accept any proposed changes; which under no circumstances, shall be less than 10 calendar days;

ii. the proposed terms under which the customer will be deemed to have accepted changes to the framework contract in accordance, unless they notify the service provider that they do not accept such changes before the proposed date of their entry into force;

iii. the duration of the framework contract;

iv. where relevant, the right of the customer to terminate the framework contract and any agreements relating to.

(l) The following information about redress:

i. any contractual clause on the law applicable to the framework contract;

ii. the availability of alternative dispute resolution procedures for the customer and the methods for having access to them.

OB-2.1.2 The information specified in Paragraph OB-2.1.1 must be provided to the customer free of charge before initiation of service.

OB-2.1.3 **(a)** A framework contract may provide for the PISP to have the right to stop the use of a payment instrument on reasonable ground relating to: the security of the payment instrument; or
(b) the suspected unauthorised or fraudulent use of the payment instrument.

OB-2.1.4 **AISPs and PISPs** must agree the basis, the time period and the manner in which the information on its intention to stop the use of the payment instrument will be provided to the customer and to the relevant licensees maintaining customer accounts.

OB-2.2 Standards for Authentication and Communication

Secure authentication

OB-2.2.1 **AISPs and PISPs must have in place a strong customer authentication process and ensure the following:**

(a) no information on any of the elements of the strong customer authentication can be derived from the disclosure of the authentication code;

(b) it is not possible to generate a new authentication code based on the knowledge of any other code previously generated; and

(c) the authentication code cannot be forged.

OB-2.2.2 The CBB will consider application of quantitative thresholds below which the strong customer authentication requirements may be simplified on a case to case basis.

OB-2.2.3 **PISPs and AISPs must adopt security measures that meet the following requirements:**

(a) the authentication code generated must be specific to the payment transaction and the payee agreed to by the payer when initiating the transaction; and

(b) the authentication code accepted by the licensee maintaining customer account corresponds to the original specific amount of the payment transaction and to the payee agreed to by the payer;

(c) a SMS message must be sent to the customer upon accessing the online portal or application and when a transaction is initiated and executed;

(d) any change to the amount or the payee must result in the invalidation of the authentication code generated.

OB-2.2 Standards for Authentication and Communication (continued)

Independence of elements of strong authentication

OB-2.2.4 AISPs and PISPs must establish adequate security features for customer authentication including the use of the following three elements:

(a) an element categorised as knowledge (something only the user knows), such as length or complexity of the pin or password;

(b) an element categorised as possession (something only the user possesses) such as algorithm specifications, key length and information entropy, and

(c) for the devices and software that read, elements categorised as inherence (something the user is), i.e. algorithm specifications, biometric sensor and template protection features.

OB-2.2.5 AISPs and PISPs must ensure that the elements referred to in Paragraph OB-2.2.4 are independent, so that the breach of one does not compromise the reliability of the others, in particular, when any of these elements are used through a multi-purpose device, i.e. a device such as a tablet or a mobile phone which can be used for both giving the instruction to make the payment and for being used in the authentication process. The CBB will consider exempting from a 3 factor authentication on a case to case basis for small value payments provided there are adequate security features.

OB-2.2.6 Where any of the elements of authentication or the authentication code is used through a multi-purpose device including mobile phones and tablets, the AISP and PISP must adopt security measures to mitigate the risk resulting from the multi-purpose device being compromised. The mitigating measures must include each of the following:

(a) the use of separated secure execution environments through the software installed inside the multi-purpose device; and

(b) mechanisms to ensure that the software or device has not been altered by the payer or by a third party or mechanisms to mitigate the consequences of such alteration where this has taken place.

OB-2.2 Standards for Authentication and Communication (continued)

Confidentiality and Integrity of Personalised Security Credentials

OB-2.2.7 AISPs and PISPs must ensure that the creation of personalised security credentials is performed in a secure environment. AISPs and PISPs must mitigate the risks of unauthorised use of the personalised security credentials and of the authentication devices and software due to their loss, theft or copying before their delivery to the payer.

OB-2.2.8 AISPs and PISPs must ensure the confidentiality and integrity of the personalised security credentials of the customer, including authentication codes, during all phases of authentication including display and transmission.

OB-2.2.9 For the purpose of Paragraph OB-2.2.8, AISPs and PISPs must ensure that each of the following requirements are met:

(a) personalised security credentials are masked when displayed and not readable in their full extent when input by the customer during the authentication;

(b) personalised security credentials in data format, as well as cryptographic materials related to the encryption of the personalised security credentials are not stored in plaintext;

(c) secret cryptographic material is protected from unauthorised disclosure.

OB-2.2.10 PISPs and AISPs must ensure that only the customer is associated with the personalised security credentials, with the authentication devices and the software in a secure manner.

OB-2.2 Standards for Authentication and Communication (continued)

Security of Communication Sessions

OB-2.2.11 AISPs and PISPs must ensure that any communication session established with the customer, and other entities, including merchants, relies on each of the following:
(a) a unique identifier of the session;
(b) security mechanisms for the detailed logging of the transaction, including transaction number, timestamps and all relevant transaction data; and
(c) timestamps which shall be based on a unified time-reference system and which shall be synchronised according to an official time signal.

OB-2.2.12 AISPs and PISPs must rely on qualified certificates for electronic seals for identification of the different parties for communication between parties.

OB-2.2.13 AISPs and PISPs must ensure that the risks against misdirection of communication to unauthorised parties in mobile applications and other customers' interfaces offering electronic payment services are effectively mitigated.

OB-2.2.14 AISPs and PISPs must ensure that, when exchanging data via the internet, secure encryption, using strong and widely recognised encryption techniques, is applied between the communicating parties throughout the respective communication session in order to safeguard the confidentiality and the integrity of the data, using strong and widely recognised encryption techniques.

OB-2.2 Standards for Authentication and Communication (continued)

OB-2.2.15 AISPs and PISPs must keep the access sessions offered by the licensee maintaining customer account, as short as possible and they shall actively terminate the session with the relevant licensee maintaining customer account as soon as the requested action has been completed.

OB-2.2.16 When maintaining parallel network sessions with the bank licensees, AISPs and PISPs must ensure that those sessions are securely linked to relevant sessions established in order to prevent the possibility that any message or information communicated between them could be misrouted.

OB-2.2.17 AISPs and PISPs, with the licensee maintaining customer accounts must include unambiguous reference to each of the following items:

(a) the customer or users and the corresponding communication session in order to distinguish several requests from the same customer or users;

(b) for payment initiation services, the uniquely identified payment transaction initiated;

(c) For confirmation on the availability of funds, the uniquely identified request related to the amount necessary for the execution of transaction.

OB-2.2.18 AISPs and PISPs must ensure that where they communicate personalised security credentials and authentication codes, these are not readable by any staff at any time. In case of loss of confidentiality of personalised security credentials under their sphere of competence, PISPs and AISPs must inform without undue delay the customer associated with them and the issuer of the personalised security credentials.

OB-2.2.19 AISPs must have in place suitable and effective mechanisms that prevent access to information other than from designated payment accounts and associated payment transactions, in accordance with the customer's explicit consent.

OB-2.2 Standards for Authentication and Communication (continued)

OB-2.2.20 **PISPs must provide the licensees maintaining customer accounts with the same information requested from the customer when initiating the payment transaction directly, unless the collection of additional information for the purposes of the provision of the payment initiation service is agreed otherwise between PISP, payer, and the licensee maintaining customer accounts.**

OB-2.3 Payment Transactions

Consent to Initiate Payment Transactions

OB-2.3.1 A payment transaction is to be regarded as having been authorised by the payer for the purposes of this Module only if the payer has given its consent to:

(a) the execution of the payment transaction; or

(b) the execution of a series of payment transactions of which that payment transaction forms part.

OB-2.3.2 For the purpose of Paragraph OB-2.3.1, such consent must be given in the form, and in accordance with the procedure, agreed between the licensee maintaining the customer account, the payer and the PISP and may be given via the payee or a PISP.

OB-2.3.3 PISP must ensure that the payer can withdraw its consent to a payment transaction at any time before the point at which the payment order can no longer be revoked under the terms of the framework contract with the customer.

OB-2.3.4 The customer may withdraw its consent to the execution of a series of payment transactions at any time with the effect that any future payment transactions are not regarded as authorised for the purposes of this section.

OB-2.3 Payment Transactions (continued)

Limits on Payment Transactions

OB-2.3.5 The PISP may agree on payment transaction limits based on its own discretion or on account of the following limitations:
(a) limits imposed by the CBB from time to time;
(b) limits imposed by any of the licensees; and/or
(c) limits imposed based on customer request.

OB-2.3.6 Subject to the framework contract, a PISP has the right to stop the use of a payment instrument on reasonable ground relating to:
(a) the security of the payment instrument; or
(b) the suspected unauthorised or fraudulent use of the payment instrument.

OB-2.3.7 PISPs must ensure that a customer to whom a payment instrument has been issued must keep safe the personalised security credentials and must:
(a) use it in accordance with the terms and conditions governing such use; and
(b) notify the PISP in an agreed manner and without undue delay on becoming aware of the loss, theft, misappropriation or unauthorised use of the payment instrument.

Fees and charges

OB-2.3.8 The AISPs and PISPs may charge fees and charges which reasonably corresponds to the PISP's costs which should be explicitly agreed in the framework contract.

MODULE	OB:	Open Banking
CHAPTER	OB-2:	Operating Rules

OB-2.4 Technology Related Requirements

OB-2.4.1 **AISPs and PIPSs must adhere to the best practices of technical standards, including for application program interfaces (APIs), electronic identification, transmission of data and web security. Technology architecture that uses "screen scarping" method must not be used.**

OB-2.4.2 AISPs, PISPs in conjunction with licensees maintaining customer accounts shall develop an open banking API standard based on a standard adopted in a leading financial centre which should be subject to independent tests, including testing in a test environment.