Version v1.1.0

30 April 2019

OPEN BANKING

Open Banking
Operational Guidelines

Disclaimer: *The contents of the Operational Guidelines ("OG") and Operational Guidelines Checklist ("OG Checklist") do not constitute legal advice. While the OG and OG Checklist have been drafted with regard to relevant regulatory provisions and best practice, they are not a complete list of the regulatory or legal obligations that apply to Participants. Although intended to be consistent with regulations and laws, in the event of any conflict with such regulations and laws, those regulations and laws will take priority. Participants are responsible for their own compliance with all regulations and laws that apply to them, including without limitation, PSRs, PSD2, GDPR, consumer protection laws and anti-money laundering regulations.*

Contents

1.0 Introduction

The Operational Guidelines ("the OG") and Operational Guidelines Checklist ("the OG Checklist") have been designed to support ASPSPs with their request for an exemption from providing a contingency mechanism. Building on the RTS-SCA, the final EBA Guidelines and the FCA's Approach documents[1] which set out criteria, guidance and information requirements for ASPSPs seeking an exemption, the OG and OG Checklist provide recommendations to help ASPSPs demonstrate compliance with these regulatory requirements.

These recommendations are designed to help deliver an effective Open Banking ecosystem, meeting the needs of TPPs in providing services to PSUs. We expect that ASPSPs who adopt the OG and OG Checklist will be in a better position to successfully demonstrate they have delivered a dedicated interface with the necessary attributes and functionality to drive competition and innovation[2].

The OG and OG Checklist will be revised in the event of changes to regulatory guidance and to support future releases of the OBIE Standard.

While this document is focused on PSD2 in-scope accounts and functionality, all of the recommendations can still be applied by ASPSPs implementing account types and functionality which are outside the scope of PSD2.

[1] The full titles of the main documents referenced throughout are:

- EBA Guidelines - Guidelines on the conditions to benefit from an exemption from the contingency mechanism under Article 33(6) of Regulation (EU) 2018/389 (RTS on SCA & CSC)
- PSRs Approach - The FCA's role under the Payment Services Regulations 2017 and the Electronic Money Regulations 2011 (December 2018 version 3)
- PS RTS Approach - Policy Statement PS18/24: Approach to final Regulatory Technical Standards and EBA Guidelines under the revised Payment Services Directive (PSD2)
- FCA request form - https://www.fca.org.uk/publication/forms/contingency-exemption-request-form-2018.pdf

[2] The decision to grant an exemption from the contingency mechanism is entirely at the discretion of the relevant Competent Authority

1.1 The Operational Guidelines

The OGs have the following objectives:

1. To provide clarity to ASPSPs to enable them to design effective and high-performing dedicated interfaces while fulfilling their regulatory obligations.
2. To ensure that TPPs have access to consistently well-designed, well-functioning and high performing dedicated interfaces.
3. To ensure that consumers and SMEs using TPP services have positive experiences that encourage them to continue to consume open banking-enabled services.

In addition, adherence to these OGs and the OG Checklist will provide the following benefits:

Exemption support: Support ASPSPs with their application to their NCA for an exemption from providing a contingency mechanism.

Lower Costs: Minimise the potential costs to a business when systems or supporting networks are down (including instances where they have not been tested appropriately).

Reduced Reputational Risk: Protect the reputation of individual participants and the Open Banking ecosystem as a whole.

1.2 The Operational Guidelines Checklist

The OG Checklist consolidates the requirements of the FCA Checklist[1] and recommendations of the OG, and helps ASPSPs identify where they are conforming to the OG. Each element of the OBIE Standard includes aspects which are either one, or a combination, of:

CMA Order: These are required by the Order and only apply to the CMA9 banks as identified in the CMA Order.

PSD2: These are either Mandatory or Optional under PSD2 (Level 1) or RTS (Level 2) texts, according to the interpretation of OBIE. Any item considered to be Mandatory under PSD2 is considered a requirement in the Open Banking Standard. ASPSPs, based on their interpretation of the legislation, should explain their rationale for deviating from the OBIE Standard to their NCA when applying for an exemption. (See e.g. Column B of the FCA's Form B[2]).

OBIE: These are items that OBIE believes would be particularly beneficial for PSUs and TPPs if implemented by ASPSPs based on consultation with a large number of stakeholders.

[1] In particular the FCA's own questions which we refer to as the FCA Checklist from https://www.fca.org.uk/publication/forms/contingency-exemption-request-form-2018.pdf which should be read alongside Chapter 17 of the PSRs Approach

[2] https://www.fca.org.uk/publication/forms/contingency-exemption-request-form-2018.pdf

OPEN BANKING

2.0 Availability and performance

The purpose of this chapter is to set out availability and performance requirements and recommendations for ASPSPs relating to EBA Guidelines 2.2, 2.3 and 2.4 and Publication of Statistics relating to Guideline 3 and FCA PSRs Approach 17.113 to 17.117.

TPPs need to be able to rely on highly available and well performing dedicated interfaces provided by ASPSPs, so that they can in turn provide reliable services to their customers.

This Chapter does not cover EBA Guideline 2.1, which states that ASPSPs "should define key performance indicators (KPIs) and service level targets, including for problem resolution, out of hours support, monitoring, contingency plans and maintenance for its dedicated interface, that are at least as stringent as those for the interface(s) made available to its own payment service users (PSUs) for directly accessing their payment accounts online." Rather, these requirements are considered in Chapters 4, 5 and 6.

In this chapter

2.1 Key Indicators for availability and performance

The following tables set out:

- The regulatory requirements, as defined by EBA Guidelines 2.2, 2.3 and 2.4.
- For each requirement, OBIE guidelines to explain how these should be calculated by ASPSPs for the dedicated interface.
- For each requirement, an OBIE recommended benchmark for the dedicated interface.

Regarding the latter, the RTS is clear that ASPSPs must *"...ensure that the dedicated interface offers at all times the same level of availability and performance, including support, as the interfaces made available to the payment service user for directly accessing its payment account online..."* and *"...define transparent key performance indicators and service level targets, at least as stringent as those set for the interface used by their payment service users both in terms of availability and of data provided in accordance with Article 36"* (RTS Arts. 32(1) and (2)).

While in most cases the availability and performance standards of an ASPSP's customer channel should be a sufficient proxy for TPP and customer expectations, parity with a poorly performing customer interface could lead to poor TPP and customer experiences and outcomes.

For this reason we believe that an effective Open Banking ecosystem needs ecosystem-wide benchmarks, referred to as the "OBIE Recommended Benchmark":

- These benchmarks are based on feedback from the developer community for what a well performing API should support to enable PSU adoption and should be achievable by ASPSPs in most cases.
- Benchmark availability and AISP and PISP response times are based on the best performing endpoints of the CMA9 in the UK at the end of 2018[1] and factor in 1000 milliseconds (ms) per megabyte (MB) to cater for larger payloads.
- Benchmarks for CBPII response times are based upon international card schemes' authorisation response times. It is noted that this benchmark would not apply to complex corporate models, but rather simple account models only.
- OBIE will review these benchmarks on a regular basis.

ASPSPs must, as per EBA/FCA requirements, ensure (at least) parity between the availability and performance of their best performing PSU interface and that of their dedicated interface.

Separately, to ensure an appropriate base level of availability and performance of the dedicated interface, ASPSPs should aim to adhere to the OBIE Recommended Benchmark, unless (in the unlikely event) that this would bring the dedicated interface below the availability and performance of the PSU interface.

[1] More information can be found here - https://www.openbanking.org.uk/providers/account-providers/api-performance/

2.1 Key Indicators for availability and performance

2.1.1 Availability

EBA Guideline 2.2 sets out a minimum of two KPIs for availability that an ASPSP should have in place for each of its dedicated interfaces. EBA Guideline 2.4 provides information on how to calculate these KPIs. The following table explains these KPIs in greater detail and provides further guidance on how they should be calculated.

TPPs may consider that a dedicated interface is only available if it is responding to all valid TPP requests a) without error messages and b) that have received a successful response from the ASPSP, for example returning the data required to be provided to an AISPs under PSD2. OBIE has catered for error messages under section 2.2.2 below, and data quality under Section 3.2 below.

Reference	Title	EBA requirement	OBIE calculation guidelines	OBIE recommended benchmark
EBA Guideline 2.2 a	The uptime per day of all interfaces	...the ASPSP should: a) calculate the percentage uptime as 100% minus the percentage downtime;	For each 24 hour period, 100% minus the total percentage downtime in that period.	A quarterly uptime of 99.5%.

2.1 Key Indicators for availability and performance

2.1.1 Availability

Reference	Title	EBA requirement	OBIE calculation guidelines	OBIE recommended benchmark

EBA Guideline 2.2 b	The downtime per day of all interfaces	b) calculate the percentage downtime using the total number of seconds the dedicated interface was down in a 24 hour period, starting and ending at midnight;
		c) count the interface as 'down' when five consecutive requests for access to information for the provision of payment initiation services, account information services or confirmation of availability of funds are not replied to within a total timeframe of 30 seconds, irrespective of whether these requests originate from one or multiple PISPs, AISPs or CBPIIs. In such a case, the ASPSP should calculate downtime from the moment it has received the first request in the series of five consecutive requests that were not replied to within 30 seconds, provided that there is no successful request in between those five requests to which a reply has been provided.
			Downtime should be calculated as follows:
			• The total number of concurrent seconds per API call, per 24 hour period, starting and ending at midnight, that any element of the dedicated interface is not available divided by 86,400 (the number of seconds in 24 hours) and expressed as a percentage.
			• The clock for unavailability should start immediately after the first 'failed' request has been received within the 30 second timeframe.
			At a minimum, downtime should be measured if:
			• Any ASPSP authorisation and/or resource server is not fully accessible and accepting all valid TPP requests as defined by EBA Guidelines 2.4c.
			• Any ASPSP downstream system required to support these API endpoints is also not responding in a way which effects the availability of the ASPSP authorisation and/or resource servers.
			• Any of the ASPSP screens and/or functionality of the PSU authentication flow is not available to enable PSUs to grant TPPs access to their account(s).
			• This should include all 5xx errors.
			• This should include both planned and unplanned downtime during each day.
			• Even if this only effects some TPPs and/or PSUs, downtime should still be reported, i.e. partial downtime should still be measured as downtime.
			• This should include any vendor/supplier failures in the case where the ASPSP has contracted the vendor/supplier to deliver a related service, e.g.
			  ◦ the ASPSP's own hosting provider,
			  ◦ any QTSP the ASPSP has selected for their own certificates,
			  ◦ a third party directory service (e.g. the OBIE Directory).
			However, this should exclude errors resulting from issues outside of the ASPSP's direct control, such as any of the following:
			• Issues with TPP software, infrastructure or connectivity.
			• Lack of response/availability from an individual QTSP resulting in the inability of the ASPSP to check validity of a TPP's eIDAS certificate, since it is the TPP who has selected the QTSP.
			The above guidelines relate only to how ASPSPs should calculate downtime. ASPSPs must be mindful of their own regulatory obligations under the PSD2 regulatory framework and eIDAS Regulation.
				A quarterly downtime of 0.5%.
				(circa 11 hours per quarter, or just under four hours per month, to allow for planned releases, updates, and also any unplanned downtime).

2.1 Key Indicators for availability and performance

2.1.2 Performance

EBA Guideline 2.3 sets out a minimum of four KPIs for performance that an ASPSP should have in place for each of its dedicated interfaces. The following table explains these KPIs in greater detail and provides guidance on how they should be calculated.

The OBIE Standard defines a number of endpoints which should be made available by ASPSPs in their dedicated interface. While all supported endpoints should be included by ASPSPs when calculating error rates, for reporting response times the consent endpoints should be ignored, as these are not considered part of the process of 'providing the information requested' to the TPP for payment initiation, account information or Confirmation of Funds.

Reference	Title	EBA requirement	OBIE calculation guidelines	OBIE recommended benchmark
EBA Guideline 2.3 (a)	PISP response time	**...the ASPSP should define, at a minimum, the following KPIs for the performance of the dedicated interface:** a) the daily average time (in milliseconds) taken, per request, for the ASPSP to provide the payment initiation service provider (PISP) with all the information requested in accordance with Article 66(4)(b) of PSD2 and Article 36(1)(b) of the RTS;	The "time taken per request" should be calculated for each day using the mean value of Time to Last Byte (TTLB) measured in milliseconds, starting from the time that each endpoint request has been fully received by the ASPSP and stopping when the last byte of the response message has been transmitted to the PISP. **The following API endpoints should be included when calculating PISP response times, for each endpoint supported by the ASPSP:** • POST /domestic-payments • GET /domestic-payments/{DomesticPaymentId} • GET /domestic-payments/{DomesticPaymentId}/payment-details • POST /domestic-scheduled-payments • GET /domestic-scheduled-payments/{DomesticScheduledPaymentId} • GET /domestic-scheduled-payments/{DomesticScheduledPaymentId}/payment-details • POST /domestic-standing-orders • GET /domestic-standing-orders/{DomesticStandingOrderId • GET /domestic-standing-orders/{DomesticStandingOrderId}/payment-details • POST /international-payments • GET /international-payments/{InternationalPaymentId} • GET /international-payments/{InternationalPaymentId}/payment-details • POST /international-scheduled-payments • GET /international-scheduled-payments/{InternationalScheduledPaymentId} • GET /international-scheduled-payments/{InternationalScheduledPaymentId}/payment-details • POST /international-standing-orders • GET /international-standing-orders/{InternationalStandingOrderPaymentId} • GET /international-standing-orders/{InternationalStandingOrderPaymentId}/payment-details • POST /file-payments • GET /file-payments/{FilePaymentId} • GET /file-payments/{FilePaymentId}/report-file • GET /file-payments/{FilePaymentId}/payment-details	An average TTLB of 750 milliseconds per response for all but file payments.

2.1 Key Indicators for availability and performance

2.1.2 Performance

Reference	Title	EBA requirement	OBIE calculation guidelines	OBIE recommended benchmark
			Continued… The ASPSP's signed response to the POST will inherently act as proof of receipt of the payment order by the ASPSP, which will enable the TPP to log a reference and the date of this receipt. Both the POST and the GET endpoints contain all information relating to the payment, which, depending on the payment type, should include reference, amount, exchange rate, charges, and status (which may change between POST and any subsequent GET). The POST endpoints above cater for the requirements of PSD2 Article 66(4)(b), RTS Article 36(1)(b), i.e. for the ASPSP to make the information available to the PISP immediately after receipt of the payment order, and the FCA PSRs Approach Paragraph 17.29, i.e. the provision of all information on the initiation of the payment transaction and all information accessible to the ASPSP regarding the execution of the payment transaction. The GET endpoints cater for the requirements of the PSRs Approach Paragraph 17.30, i.e. for the ASPSP to provide confirmation to the PISP that payment initiation has been successful, in order to enable the PISP to provide this information to the PSU. We note that because different endpoints will have different payload sizes for request and response (especially relevant for file payment endpoints involving large files), and in order to facilitate a 'like for like' comparison with PSU interfaces, OBIE recommends that ASPSPs also report on the average time per megabyte (MB). This can be calculated by dividing the total response time in milliseconds by the total payload response size in MB, across all API calls for all API endpoints for each day.	

2.1 Key Indicators for availability and performance

2.1.2 Performance

Reference	Title	EBA requirement	OBIE calculation guidelines	OBIE recommended benchmark
EBA Guideline 2.3 (b)	AISP response time	b) the daily average time (in milliseconds) taken, per request, for the ASPSP to provide the account information service provider (AISP) with all the information requested in accordance with Article 36(1)(a) of the RTS;	The "time taken per request" should be calculated for each day using the mean value of Time to Last Byte (TTLB) measured in milliseconds, starting from the time that each endpoint request has been fully received by the ASPSP and stopping when the last byte of the response message has been transmitted to the AISP. **The following API endpoints should be included when calculating AISP response times, for each endpoint supported by the ASPSP:** • GET /accounts • GET /accounts/{AccountId} • GET /accounts/{AccountId}/balances • GET /balances • GET /accounts/{AccountId}/transactions • GET /transactions • GET /accounts/{AccountId}/beneficiaries • GET /beneficiaries • GET /accounts/{AccountId}/direct-debits • GET /direct-debits • GET /accounts/{AccountId}/standing-orders • GET /standing-orders • GET /accounts/{AccountId}/product • GET /products • GET /accounts/{AccountId}/offers • GET /offers • GET /accounts/{AccountId}/party • GET /party • GET /accounts/{AccountId}/parties • GET /accounts/{AccountId}/scheduled-payments • GET /scheduled-payments • GET /accounts/{AccountId}/statements • GET /accounts/{AccountId}/statements/{StatementId} • GET /accounts/{AccountId}/statements/{StatementId}/file • GET/accounts/{AccountId}/statements/{StatementId}/transactions • GET /statements We note that because different endpoints will have different payload sizes for request and response, and in order to facilitate a 'like for like' comparison with PSU interfaces, OBIE recommends that ASPSPs also report on the average time per megabyte (MB). This can be calculated by dividing the total response time in milliseconds by the total payload response size in MB, across all API calls for all API endpoints for each day.	An average TTLB of 750 milliseconds per response, or per page of results for up to 100 records for larger payloads. In practice, all but transactions and statements are likely to be small payloads without pagination.

2.1 Key Indicators for availability and performance

2.1.2 Performance

Reference	Title	EBA requirement	OBIE calculation guidelines	OBIE recommended benchmark
EBA Guideline 2.3 (c)	Confirmation of Funds (CoF) response time (CBPII and PISP)	c) the daily average time (in milliseconds) taken, per request, for the ASPSP to provide the card-based payment instrument issuer (CBPII) or the PISP with a 'yes/no' confirmation in accordance with Article 65(3) of PSD2 and Article 36(1)(c) of the RTS;	The "time taken per request" should be calculated for each day using the mean value of Time to Last Byte (TTLB) measured in milliseconds, starting from the time that each endpoint request has been fully received by the ASPSP and stopping when the last byte of the response message (i.e. the 'yes/no' conformation) has been transmitted to the CBPII or PISP. **The following API endpoints should be included when calculating CoF response times for CBPII:** • POST /funds-confirmations **The following API endpoints should be included when calculating CoF response times for PISP:** • GET /domestic-payment-consents/{ConsentId}/funds-confirmation • GET /international-payment-consents/{ConsentId}/funds-confirmation • GET /international-scheduled-payment-consents/{ConsentId}/funds-confirmation	An average TTLB of 300 and a max of 500 milliseconds per response. This benchmark would not apply to complex corporate models, but rather simple account models only.
EBA Guideline 2.3 (d)	Daily error response rate	d) the daily error response rate – calculated as the number of error messages concerning errors attributable to the ASPSP sent by the ASPSP to the PISPs, AISPs and CBPIIs in accordance with Article 36(2) of the RTS per day, divided by the number of requests received by the ASPSP from AISPs, PISPs and CBPIIs in the same day.	It is not possible for ASPSPs to respond to TPPs with an error message where no TLS session has been established. However ASPSPs should still be able to respond, measure and report on errors relating to all OIDC endpoint calls and all functional API calls relating to the OBIE Standard. The error response rate should be calculated as the total number of all 5xx HTTP status codes from all API endpoints per day, divided by the total number of TPP API requests received across all of these endpoints in the same day, and expressed as a percentage. Errors based on 4xx HTTP status codes are largely attributable to TPP or PSU actions or failures, and hence should not be included here. Cases where 2xx HTTP status codes are returned, but where the data in the response payload is not correct are covered in section 3.1 below.	An average of 0.5% across all endpoints

2.2 Publication of statistics

EBA Guideline 3.1 requires that ASPSPs *"... provide its competent authority with a plan for publication of daily statistics on a quarterly basis on the availability and performance of the dedicated interface as set out in Guidelines 2.2 and 2.3, and of each of the interfaces made available to its own PSUs for directly accessing their payment accounts online, together with information on where these statistics will be published and the date of first publication..."*

In addition, the FCA PSRs Approach Chapter 13 requires ASPSPs to report these statistics to the FCA on a quarterly basis.

These statistics should be completed for each dedicated interface. In the case where an ASPSP has one dedicated interface per brand, then the ASPSP should publish a separate report for each brand. However where several brands share the same interface, then the ASPSP should only need to publish one report. In the case where an ASPSP maintains different versions of their dedicated interface in parallel (e.g. to support different versions of the OBIE Standard), then these should be considered as separate dedicated interfaces and published separately, as they may have different levels of availability and performance.

2.2 Publication of statistics

2.2.1 Reporting for PSU interfaces

As per the EBA Guidelines, the ASPSP must publish statistics for each PSU interface. Therefore an ASPSP with a separate website and mobile app for consumer accounts and a separate website and mobile app for business accounts may need to report separately to cover each of the four PSU interfaces (which may still be within a single report) .

In this regard, ASPSPs are only required to report on PSU interface for PSD2 in-scope accounts and regarding PSD2 in-scope functionality (i.e. initiation of a credit transfer payments and/or accessing account and transaction information). In order to enable a 'like for like' comparison, OBIE recommends the following guidance for calculating each element in regard to PSU interface availability and performance:

- **Uptime:** 100% minus the total percentage downtime for each day.
- **Downtime:** The total time in seconds for each day when any element of the PSU interface is not accessible by the PSU in the process of accessing their PSD2 in-scope account, and in order to access PSD2 functionality. This should be divided by 86,400 (the number of seconds in 24 hours) and expressed as a percentage. PSU accounts which have been blocked by the ASPSP should not be counted as downtime, as it is the downtime of the service, and not the individual PSU's access, which is relevant here.
- **PISP response time:** The average time taken in milliseconds from when a PSU clicks on a button or link to initiate a payment (i.e. after they have supplied all details and clicked “confirm payment”) to when the PSU receives either a confirmation screen or error message to confirm the status of the payment initiation. This should be the average for all PSU payments initiated each day for each PSU interface. OBIE recommends that the time is reported based on the time taken for the page/screen which contains the confirmation/error message to fully load.
- **AISP response time:** The average time taken in milliseconds from when a logged in (i.e. authenticated) PSU clicks on a button or link to access any PSD2 in-scope payment account information on their account (e.g. list of accounts, balance for an account, page/screen of transactions) to when the page/screen displaying this information has fully loaded. Where this information is displayed immediately and automatically after login, this time should be measured from when the ASPSP has accepted the last factor of the PSU’s authentication (i.e. the load time of the first page/screen after authentication is complete). This should be the average for all pages/screens loaded each day for each PSU interface. OBIE recommends that the time is reported based on the time taken for the page/screen which contains the confirmation/error message to fully load.
- **Confirmation of Funds response time:** There is no direct comparison for CBPII and PISP confirmation of funds in a PSU interface, hence this column should be left blank.
- **Error response rate:** As per row 23 in the EBA consultation feedback table, this column is not required for a PSU interface and should also be left blank.

2.2 Publication of statistics

2.2.2 ASPSP reporting template

OBIE has included a template that ASPSPs using the OBIE Standard might find useful in preparing their information for publication and reporting to the FCA (or other CA) from September 2019:

OBIE ASPSP Reporting Template v1.1

Whilst ASPSPs are only required to publish statistics on their website and submit to FCA every quarter, OBIE recommends that non-CMA9 ASPSPs submit these reports (all completed Report Tabs) and also the detailed workings (the Data Tab) using this template to OBIE on a monthly basis. This will enable OBIE to track overall health and growth of the Open Banking ecosystem.

Where ASPSPs support more than one major or minor API version in production, each version must be reported separately. For example, v3.0 and v3.1 must be reported separately. However patches, for example v3.1.1, should be reported as aggregate together with the relevant major or minor release (i.e. together with v3.1).

For the avoidance of doubt, the reports that the CMA9 ASPSPs are mandated to provide to OBIE are detailed in a separate MI template and not covered within this document.

2.2.3 TPP reporting

OBIE encourages TPPs to report statistics on availability and performance to OBIE. Whilst there is no EBA/FCA regulatory requirement, OBIE would find this information very useful in providing a balanced view of the overall health of the Open Banking ecosystem. The format and method of this is still to be confirmed and sits outside this document.

OPEN BANKING

3.0 Dedicated interface requirements

This chapter provides guidance on the overall expectation for ASPSPs to demonstrate that their dedicated interface has been designed and tested in line with EBA requirements; that is has been appropriately stress tested; and to evidence wide usage by TPPs.

OBIE deems this essential in order for ASPSPs to successfully deliver the necessary functionality for the Open Banking ecosystem and to facilitate the creation of seamless customer experiences, which do not constitute obstacles for the provision of TPP services.

OBIE considers that the implementation of effective design and testing (including stress testing) and the creation of obstacle-free customer journeys will provide TPPs with the confidence to offer their service to their customers with the knowledge that an ASPSP's dedicated interface will support rather than hinder the provision of their service.

The EBA Guidance means that ASPSPs must ensure consistent engagement with TPPs within their design and testing processes so that issues are identified and rectified as early as possible. Robust stress testing will ensure that the dedicated interface is capable of dealing with not only anticipated demands but with higher-than-usual peak periods. Wide usage of the dedicated interface is required to show that it is capable of supporting a diverse set of TPP business models and use cases.

OBIE has also briefly outlined what ASPSPs need to consider so as not to present obstacles to TPPs. This is covered more extensively within the Customer Experience Guidelines[1].

[1] https://www.openbanking.org.uk/wp-content/uploads/Customer-Experience-Guidelines-V1-1.pdf

In this chapter

3.1 Design and Testing

3.1.1 The OBIE Standard

The OBIE Standard have been developed over a period of 18 months in collaboration with nine of Europe's largest financial institutions as well as 500+ representatives from other ASPSPs, TPP communities, PSD2 and consumer stakeholder groups, and prominent fintech leaders.

The collaborative and transparent development process has involved over 50 workshops and an online feedback process, giving stakeholders the opportunity to contribute to ensure that their regulatory requirements have been considered for the widest possible coverage of business models. As such, when ASPSPs adopt the OBIE Standard without deviation, they can refer to the fact that there was extensive consultation during the development of the OBIE Standard as an additional tool to support the design and testing requirement.

In the UK, the FCA will base its assessment of whether the exemption criteria are met on a completed contingency exemption form. FCA-regulated ASPSPs are required to complete this (in particular the second half Form B[1]) by providing the details of functional and technical specifications that they have implemented for each relevant regulatory requirement and a corresponding summary describing how their implementation satisfies the requirement, as well as any deviations, where applicable.

We note that it is ultimately in the discretion of each NCA to determine whether or not exemption criteria are met when assessing applications for an exemption.

[1] Cf. https://www.fca.org.uk/publication/forms/contingency-exemption-request-form-2018.pdf

3.1 Design and Testing

3.1.2 Proving conformance

OBIE provides a suite of testing tools which are designed to help ASPSPs test whether or not their API interface meets the OBIE Standard. ASPSPs who use these tools will be in a good position to able to demonstrate to NCAs that they have correctly followed and implemented the OBIE Standard[1].

Functional Conformance: This suite contains a large number of test cases, which cover all functional API request, response and error codes, to ensure that the API interface is conformant to the OBIE specifications for AISP, PISP and CBPII use cases. This tool also provides a mechanism by which ASPSPs can publish details of the specification of their dedicated interface.

Security Profile Conformance: This suite includes test cases for the Open Banking Security Profile and the following Open ID Foundation profiles: redirect (FAPI profile), decoupled (CIBA profile), and TPP on-boarding (Dynamic Client Registration).

CEG

Customer Experience Guidelines Checklist: This tool allows ASPSPs to provide evidence of conformance to the Customer Experience Guidelines.

OG

Operational Guidelines Checklist: In combination with the NCA submission, ASPSPs should use this checklist to provide the NCA with a summary of the results of the testing, including the identification of weaknesses and a description of how these weaknesses have been addressed.

OBIE will also provide a certification service for each of the four areas above. This service will include OBIE's validation that the conformance tools/checklists have been run/completed satisfactorily to indicate conformance to the OBIE Standard. While the tools can be run in a test/pre-production environment, certification will be against production environments unless otherwise agreed by OBIE.

ASPSPs who run these tools and obtain a certification against their production environment will mitigate against scenarios where the dedicated interface returns 2xx HTTP status codes, but the responses contain missing, badly formed or incorrect data.

[1] While running the tools successfully will produce useful evidence, an NCA may still require further evidence to ascertain whether or not an ASPSP has correctly implemented the OBIE Standard

3.1 Design and Testing

3.1.3 Testing facility

ASPSPs are required to provide a Testing Facility to allow authorised and pre-authorised[1] TPPs to undertake connection and functional testing of their products and services using non-PSU (i.e. “dummy”) data. The issues and problems which are identified within this testing process, as well as feedback and engagement from the TPP community, are useful for ASPSPs in alerting them to potential issues within testing that may also be encountered within the production environment. This can be used to identify and address issues early on. ASPSPs will be required to provide details and information on the outputs of their testing to their NCA as part of their application for an exemption.

This facility should[2] provide an accurate reflection of the live environment, and give TPP developers access to the following, with reference to EBA Guideline 6.5:

- **Functionality:** The facility should include all functionality of the production interface relating to AISP, PISP and CBPII use cases. This functionality should work in an equivalent or representative way to the production interface including negative use cases and error codes.
- **Security:** The facility should use the same security profile/model and be configured in the same way as that which protects the production APIs.
- **On-boarding:** The facility should replicate the on-boarding process of the ASPSP's production facility, including TPP on boarding and the exchange of certificates for identification and message signing.
- **Certificates:** The facility should allow the use of both test certificates (which have the same format/structure as eIDAS certificates) and production eIDAS certificates, so that TPPs can replicate the functionality of QSEALs and/or QWACs relating to the exchange of certificates for identification and message signing, before and after they have obtained a production eIDAS certificate.
- **Test data:** The facility must not include any real PSU data (RTS Art. 30(5)). The volume and variance of data should be sufficient to support all technical and functional testing including pagination (where this is supported in the dedicated interface).
- **Test accounts:** The facility should provide TPPs with a number of test accounts that enable the functionality and access to data that real PSUs will experience in production.

[1] TPPs that have applied for authorisation with their NCA and are waiting for approval

[2] For the avoidance of doubt, the following are all recommendations only and optional for ASPSPs, unless we are referring to direct regulatory guidance

3.1 Design and Testing

3.1.3 Testing facility

- **Authentication:** The facility should enable TPPs to use 'headless authentication', i.e. authentication which does not require a PSU to be present, therefore enabling multiple tests to be run in succession via automated scripts. However, the Final EBA Guidelines have identified a new item "Guideline 6.5.(g) - the ability of PISPs and AISPs to rely on all the authentication procedures provided by the ASPSP to its PSUs". Therefore ASPSPs must allow TPPs to test all authentication procedures[1] provided to its PSUs, but ideally ASPSPs should NOT prevent 'headless authentication' testing to be conducted by the TPP as well. This could be catered for by ASPSPs either:

  a) allowing TPPs to test both headless and PSU authentication procedures in the same facility;

  b) providing a separate testing facility in order to test all authentication procedures; or

  c) allowing TPPs to test PSU authentication procedures in a production environment using their own and/or test accounts.

- **Availability and performance:** The facility is not expected to handle production volumes (i.e. is not expected to be used by ASPSPs or TPPs for stress testing), however, it should have sufficient availability, capacity, performance and other characteristics to facilitate effective and realistic connection and functional TPP testing.

- **Readiness:** The facility must enable TPPs to start testing their technical solutions at least six months prior to the application date of the RTS (or, if the launch of the ASPSP's dedicated interface takes place after the application date of the RTS, six months prior to the launch date).

- **Ongoing access:** The facility should remain as an ongoing facility and to support future development or changes to the dedicated interface at least 3 months prior to implementation of such changes.

- **Support:** The facility should have an appropriate level of support to enable communication of problems or issues by TPPs to ASPSPs and to provide efficient and effective solutions.

- **Documentation:** ASPSPs must publish externally a summary of the specification of the testing facility on their website including access details and test coverage.

The testing facility should thereby enable TPPs to successfully execute full API journeys to support their proposition with the expectation that they will be able to use the same code base when connecting to the ASPSP's production interface. In particular, this facility must ensure the API interface meets the requirements of a stable and secure connection, and the ability to exchange eIDAS and/or testing certificates. The OBIE Standard is published on the Open Banking website

[1] Participants should note the EBA feedback 103 in their final Guidelines – "Where an ASPSP is developing its authentication processes to meet SCA requirements by 14 September 2019, the EBA acknowledges that this SCA functionality may not be fully ready for testing by March 2019. However, **the testing facilities should enable AISPs and PISPs to test the planned SCA scenarios, so they can accommodate these in their software and applications**" [our emphasis]

3.1 Design and Testing

3.1.4 Publishing specification details

ASPSPs that use the OBIE Standard, or any other market initiative, should publish the details of the specifications on their website six months prior to the publication date in the RTS (or, if the launch of the ASPSP's dedicated interface takes place after the application date of the RTS, six months prior to the launch date). Should an ASPSP deviate from the Market Initiative they have adopted, they should inform their NCA with details of what changes they have made and an explanation of the rationale for the deviation.

Implementations of the specifications should be machine readable, so that TPPs can automate discovery, and include the following details by brand/product:

Connection details (including all technical and business processes required to connect).

Authentication flows supported (e.g. redirect, decoupled).

Methods of authentication available to PSUs (e.g. OTP via SMS, Fingerprint etc. and how this varies by device).

Functionality and data elements for each AISP, PISP and CBPII endpoint, including which optional elements are/are not provided.

Should any of these details change at any time, the ASPSP should notify TPPs by updating their website (e.g. through a change log) as detailed in Chapter 5.

3.2 Stress Testing

ASPSPs should conduct stress testing of their API interface as follows:

- **Environments:** Stress testing does not need to take place on the testing facility. However, stress testing should either be conducted on the production interface (and underlying production systems) and/or staging/pre-production systems which have similar infrastructure, so there can be certainty that the test results will represent what will happen in a real-word scenario.

- **Realistic scenarios and loads:** Testing should cover a range of realistic test cases and be for realistic duration and at realistic volumes, based on predicted volumes in six months' time. The actual data used for these tests is not relevant (i.e. whether this is test or production data), since this must not be disclosed in any test results submitted. Testing should take place from external networks which replicate the usage patterns expected in the real-world (e.g. from third party applications).

- **Availability and frequency:** A separate facility for stress testing does not need to be permanently available. However, stress testing should be conducted at least every six months and also in any of the following cases:

  - Prior to application to the NCA for an exemption.
  - In the event of any failures or reduction of service levels below those required regarding performance and availability KPIs.
  - In the event of any infrastructure or implementation changes (e.g. release of new API versions), which may affect performance.
  - In the event of any significant increase in predicted usage volumes.

3.3 Wide Usage

The Final EBA Guidelines have clarified that the wide usage requirements not only include the number of TPPs that make use of the dedicated interface but also the number of successful responses of ASPSPs to TPP requests the number of available TPPs and the results of testing, including the resolution of any issues that have been identified.

For the purposes of showing TPP involvement in the design of the dedicated interface, as per Section 3.2.1, we believe that given the level of engagement with TPPs in the design of the OBIE Standard, that an ASPSP implementing them as designed (i.e. without deviation) can refer to this as one source of supporting evidence.

For the matter of testing, this will need to be done on an individual ASPSP basis. In the development of the OBIE Technical Standard, the information sharing between TPPs and ASPSPs has been extremely valuable for both parties. Based on this, we are convinced that without extensive TPP input a dedicated interface of sufficient quality cannot be built, and therefore strongly endorse the EBA's requirements here i.e. three months of live production for TPPs to provide services to their customers (noting this can run concurrently with testing). Given this, we would note the changes made to the final EBA Guidelines regarding wide usage and "widely used" and the types of evidence NCAs are required to consider to assess under EBA Guideline 7.1.

If any ASPSP is unable to find TPPs with which to design and test their interfaces, we would encourage them to contact OBIE and we will attempt to find appropriate TPP partners. OBIE provides a 'buddying' service for enrolled ASPSPs to facilitate this. ASPSPs should not rely solely on the engagement of TPPs in the development of the OBIE Standard as proof of wide usage without evidence to show that the production environment was available for three months and significant effort was made to encourage TPPs to use the dedicated interface (as per EBA Guideline 7.1(b)).

3.3 Wide Usage

ASPSPs should provide detailed evidence to demonstrate wide usage, over and above TPP numbers (e.g. in the form of research, testimonials or reviews from TPPs). For example:

- Testimonials from TPPs who have been involved with testing to confirm they are satisfied with the testing facility before moving to production.
- Description of major discrepancies between the numbers of TPPs involved in testing and production and their reasons for such discrepancies.
- Testimonials from TPPs who have used the dedicated interface for three months to confirm they are satisfied with the interface (i.e. with no significant ongoing defects).
- The number of requests submitted by TPPs using the dedicated interface that have been successfully responded to by an ASPSP.
- Details of communication to TPPs relating to availability for use of the dedicated interface.

OBIE notes that the results of testing related to issues and problems that were identified, including the resolution of those problems, will also be a factor that NCAs may consider for the purposes of assessing if an ASPSP has demonstrated 'wide usage' of their implementation.

When submitting evidence for an exemption application, ASPSPs could consider providing the details of contacts at TPPs that have been involved in testing when they have been given permission from the TPP to verify the information provided by the ASPSP.

3.4 Obstacles

EBA Guideline 5 places a requirement on ASPSPs to ensure that their dedicated interface does not create obstacles for the provision of services by PISPs, AISPs and CBPIIs.

Implementation of the OBIE Technical Specifications and Security Profiles, together with use of the conformance tools to test and validate conformance, will help ASPSPs remove technical obstacles for TPPs. Furthermore, the Customer Experience Guidelines and Customer Experience Guidelines Checklist (the CEG) have been created to support this requirement from the perspective of the customer journey implemented by the ASPSP for their dedicated interface(s).

The Operational Guidelines and the Operational Guidelines Checklist (this document) contain additional requirements and recommendations for ASPSPs which, if implemented, can be utilised to further reduce obstacles relating to the overall performance and functionality of the ASPSP's interface.

The combination of the CEG and the OG can be used to support the relevant requirements of Guideline 5 and assist an ASPSP's application for an exemption.

ASPSPs should also give consideration to the "user experience" for a TPP in its direct interactions with ASPSPs, such as dynamic client registration or communication of changes to specifications.

OPEN BANKING

4.0 Problem resolution

This chapter outlines the policies, procedures and systems that an ASPSP should create and embed in order to demonstrate effective problem resolution for TPPs using their dedicated interface and test facility. It focuses on issues that specifically impact TPPs, as set out in the RTS and EBA Guidelines.

RTS, Art 33(6) sets out the conditions that an ASPSP is required to meet in order to obtain exemption from the obligation to provide a contingency mechanism. RTS, Art 33(6)(d), in particular, requires ASPSPs to ensure that any problems with their dedicated interface are resolved without undue delay.

The EBA has outlined the practicalities of the RTS provisions in EBA Guideline 8. More specifically, an ASPSP must submit information to their NCA which demonstrates they have the applicable systems and procedures in place for tracking, resolving and closing problems, as well as an explanation of problems which were not resolved within its relevant service level targets. The PSRs Approach (17.172) has clarified that this explanation must include problems which occurred within the context of both testing and production of the dedicated interface.

In this chapter

4.1 Procedures, processes and systems for problem resolution

4.1.1 Effective resolution of problems

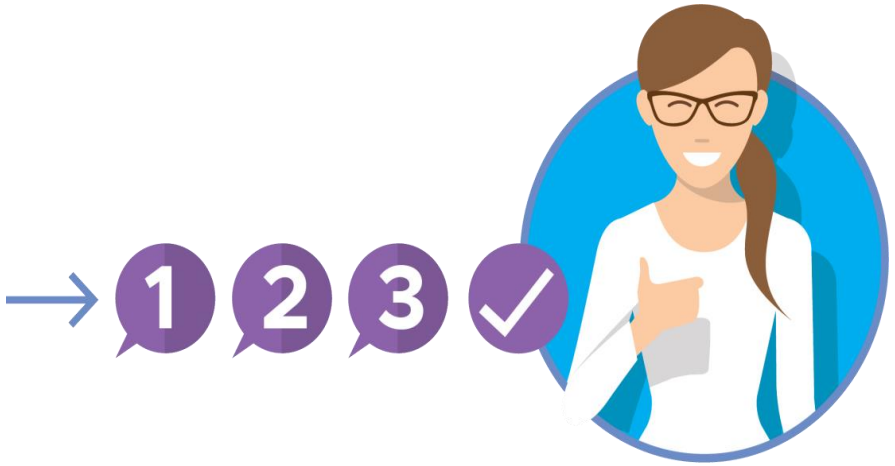
An ASPSP should create documentation to clearly outline the policies, processes and systems it has in place for problem resolution and its respective service level objectives. This framework should enable the effective resolution of TPP issues and therefore cater for problems that relate specifically to a TPP's use of an ASPSP's dedicated interface and test facility.

When a TPP encounters a problem with an ASPSP's dedicated interface, it could have a direct impact on a TPP's ability to provide its service, which in turn has the potential to cause:

- loss of business;
- reputational risk;
- additional resource requirement; and
- negative outcomes for customers.

Accordingly, it is important that an ASPSP's problem resolution framework resolves problems efficiently to enable TPPs to provide a continued, uninterrupted service to their customers. An ASPSP should review its existing problem resolution framework and associated service level targets for its PSU interface and consider if, in certain circumstances, it needs to go beyond the service levels for resolving problems with its own PSU interface.

We recommend that ASPSPs use OBIE's Support Services (see 4.3) to assist with the notification of problems (and any change) that may impact a TPP. Any problems or changes that may impact a TPP will be added to the central noticeboard facility to inform all ecosystem participant



4.1 Procedures, processes and systems for problem resolution

4.1.2 Online support

ASPSPs should provide FAQs, which address areas that may be specific to TPPs such as technical advice or test facility guidance. They should also consider a means of identifying recurring questions or user-error issues so these can be collated into FAQs to support the early resolution of problems.

Problem resolution documentation, FAQs, contact details, opening times and out of hours support should be published and easily accessible in one collective area on the ASPSP's website.

4.1.3 Ticket management process

ASPSPs must ensure they have a functioning ticket management system which enables them to respond to issues and problems raised within clearly defined service level targets. A successful problem resolution framework will enable the efficient identification and resolution of problems which specifically impact TPPs. The system for raising and reporting on tickets should be transparent in order to fully inform users and engender trust across the ecosystem.

The ticket management process should categorise problems as and when they are reported and track the progress of each ticket until the point of closure. It should also enable an ASPSP to identify which problems relate to the operational use of the dedicated interface and the test facility. Where test facility problems have been raised by AISPs, PISPs and CBPIIs and resolved, this can be provided to the dedicated interface has been designed and tested to the satisfaction of TPPs.

4.1 Procedures, processes and systems for problem resolution

4.1.4 Tickets

All tickets should be given priority ratings and these ratings should factor in the severity of the impact on the TPP. We recommend that ASPSPs consider incorporating the following impact assessment into their ASPSPs ticket management process.

High

Business critical issue - represents a complete loss of service or a significant feature that is completely unavailable, and no workaround exists (first response SLA - one hour).

Med

Degraded service issue - includes intermittent issues and reduced quality of service. A workaround may be available (first response SLA - four hours).

Low

General issue – cosmetic issues which include product questions, feature requests and development issues in staging environments (first response SLA - 24 hours).

Ticket fields should include mandatory and drop down options to assist in efficiently identifying which level of support a TPP requires. This should include a field to allow the TPP to select an initial priority rating. The tickets should be detailed and structured so that they contain sufficient granularity that the ASPSP is able to allocate appropriate priority level.

When considering and reporting problems related to testing, ASPSPs must take into account the categories, set out in the EBA Guideline 6.5 as well as, problems raised in functional testing (RTS. Article 30(5)) and ensure problems raised within these categories are resolved within the relevant service level targets, as well as, record any problems which are not resolved within those targets. ASPSP should also the use this process to identify problems raised in live use of the dedicated interface.

OBIE recommended ticket-fields include:

- Name of reporting organisation
- Name and contact details of contact at the reporting organisation
- Date ticket raised
- Problem type/category
- Details of the problem, including an indication of the likely impact for the TPP
- Name of ASPSP and brand (if applicable)
- ASPSP environment impacted (test or production)
- Severity, as defined by TPP (if applicable)
- Severity, as defined by ASPSP
- Log of all updates from TPP and ASPSP
- Start time/date the change/fix is anticipated to take effect and the end date/time (if applicable)
- Date closed

4.1 Procedures, processes and systems for problem resolution

4.1.5 Problem mitigation and escalation process

There may be cases where a problem cannot be entirely rectified within the SLA. In such cases, workarounds and interim solutions should be considered and implemented, if possible. Problems like bugs or security issues are likely to impact the wider user group and therefore ASPSPs should create an accessible web page or communication tool to give advance notice of relevant information to TPPs.

Where workarounds or interim solutions are identified, these should also be shared as soon as possible. The ASPSP should decide the appropriate level of detail required for the communication.

Where a ticket exceeds the required SLA or in the event that a TPP does not agree that a problem can be closed, the TPP should be informed of the next steps available. This will include an additional point of escalation within the ASPSP and any other external channels of escalation that the user should be made aware of. This information should be available on the ASPSP's website and the ASPSP should inform the TPP of the next steps in the event that an SLA is not met.

4.1.6 Report generation and audit trail

ASPSPs should also regularly review any outstanding tickets that have exceeded their SLA and prioritise those with the greatest impact on the TPP. This rationale should be recorded within the problem resolution policy.

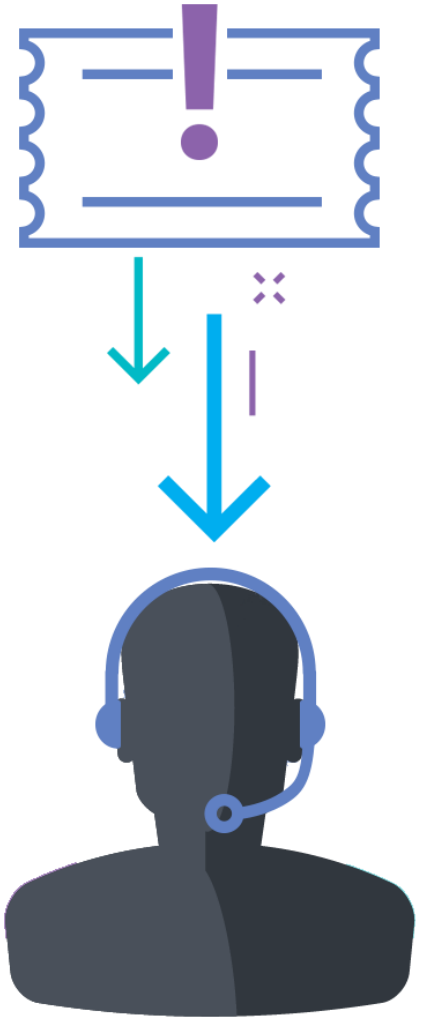
Statistical data on how many problems are logged, within different categories of severity and what percentage, if any, were not dealt with within the service level targets should be produced on a regular basis.

The ticket management process should record the progress of each ticket including the date on which a problem is raised through to closure. The historical log should then be used to evidence an audit trail of effective problem resolution.

4.2 OBIE Support

OBIE Service Desk provides participants with a supplementary ticket management process and supports ASPSPs in communicating problems to ecosystem participants via the noticeboard. ASPSPs are recommended to use the OBIE Service Desk which may provide additional evidence of an ASPSP's effectiveness in resolving problems.

The OBIE Dispute Management System (DMS) is a communication platform that helps organisations to collectively manage enquiries, complaints and disputes relating to PSUs, fairly and effectively. Version 2 of this platform (due in 2019) will allow all enrolled organisations to communicate with each other in a secure and timely manner. ASPSPs are encouraged to sign up to the platform to ensure efficient resolution of enquires, complaints and disputes relating, but not limited to, requests for information or exchange of information, requests for a redress repayment and complaints forwarding.



OPEN BANKING

5.0 Change and communication management

This chapter outlines various change scenarios that may impact TPPs and provides guidance for an ASPSP to consider when implementing a change and communicating to TPPs.

Any change that may impact a TPP's ability to deliver its services has the potential to cause a loss of business, reputational risk or to add additional resource cost to the TPP and result in a negative outcome for their customers. As such, the ability to identify the potential impact that proposed changes may have and to communicate those changes to TPPs, is key to a successful Open Banking ecosystem.

The information that an ASPSP should include in its communication to a TPP is listed at 5.4 Notification of a change.

In this chapter

5.1 Downtime

Downtime is defined in Section 2.1.1.

Planned downtime, by its nature, is something that an ASPSP anticipates and therefore is able to give advance notice to TPPs. It is not generally possible to give advanced notice of unplanned downtime, but ASPSPs should give notice as soon as they are aware of the downtime. The impact of any downtime can be minimised by an ASPSP informing TPPs as soon as the downtime is anticipated, when it takes effect and as soon as the service is reinstated. ASPSPs should therefore provide notice of downtime notifications which should be published on their own website or developer portal. When providing notifications, ASPSPs should provide a specific time period, so TPPs are aware that the dedicated interface will be unavailable for that time, or upon a subsequent notification to confirm that the service has been reinstated sooner than anticipated.

The final EBA Guidelines do not distinguish between planned and unplanned downtime. As such, when an ASPSP engages in planned downtime activities, these must be considered within the context of their obligations to ensure that their dedicated interface targeted levels of availability are at least as stringent as those for the PSU interface, including maintenance, problem resolution, out of hours support, monitoring and contingency plans. Planned downtime should not therefore be implemented in a way that it could impact the required target service levels for the dedicated interface.

OBIE Support Services can assist ASPSPs with the dissemination of downtime information to the wider Open Banking ecosystem via its central noticeboard facility**.** ASPSPs can provide advance notice for future planned downtime and submit real time updates related to downtime (planned or unplanned) that currently impact TPPs and the subsequent reinstatement of service. It is not expected that ASPSPs raise tickets for very short lived periods of unplanned downtime (e.g. when full service is likely to be restored before the ticket has been raised), although all downtime should be reported as per section 2 above.

Planned downtime should be given with at least five business days' prior to the event. Apart from cancelling the planned downtime, no changes should be made to the planned downtime notification within the five business day period. Where practical, ASPSPs should give advance notice via their own website, developer portal or OBIE of any planned downtime one calendar month in advance.

In the event that the interface does not offer at least the same level of availability and performance as the PSU interface(s), if there is unplanned downtime, or if there is a system breakdown, ASPSPs are required to have 'contingency measures' in place which include a strategy and communication plan to inform the TPPs of measures being undertaken to restore the system and a description of immediately available alternate options that TPPs may have during this time.

ASPSPs should make this plan available to TPPs (e.g. on their website or developer portal) so that they know in advance what to do in the event of unplanned downtime.

5.2 Implementation of a new OBIE Standard

The OBIE Standard will continue to evolve over time to cater for potential regulatory changes/clarifications, agreed Open Banking roadmap requirements and approved changes (which may include adding new functionality, fixing defects, and errata). Where possible, OBIE will schedule new versions of the Standard so that all participants can plan ahead and build new APIs to this plan, this will therefore reduce development and support costs for all participants and increase adoption.

5.2.1 Types of release and version numbering:

Release type	Description	Version numbering
Major	Significant breaking changes - which may require substantial implementation effort for ASPSPs and will cause existing TPP applications to fail) until TPPs also implement changes.	v1.0.0, v2.0.0, etc
Minor	Minor breaking changes – may require some implementation effort for ASPSPs and will cause existing TPP applications to fail until TPPs also implement change.	v1.1.0, v1.2.0, etc
Patch	Can include any non-breaking change, as well as errata and clarifications, which will not force TPPs to implement any changes.	v1.1.1, v1.1.2, etc
Release Candidate	Pre-release versions of any forthcoming patch, minor or major release. To enable OBIE to publish regular updates based on review and feedback.	v1.0.0-rc1, v1.0.0-rc2, etc

The version numbering above can apply to any individual component of the Standard. For example, the latest published API Specifications at a point time could be v3.1.1, and the latest published Customer Experience Guidelines (CEG) could be v1.2.0.

Within each, component, individual resources or functionalities can also change version numbers independently. For example, the latest Account and Transaction API Specification can be v3.1.1 and, within this, the /transactions resource can be v3.2.0. In this case, this resource has introduced a minor breaking change. And this may require one or more sections/sub-sections of the CEG to be updated to v1.2.1 or v1.3.0.

The above version numbering approach enables OBIE to introduce changes to the Standard incrementally, but at the same time reducing the need for ASPSPs and TPPs to make any unnecessary changes.

5.2 Implementation of a new OBIE Standard

5.2.2 Introducing change

The following apply:

- It is up to ASPSPs to take their own position of which version of each component of the Standard they chose to implement in order to meet both regulatory and commercial requirements.
- As per RTS Article 30(3), ASPSPs must publish technical specification documentation for their dedicated interface, at least six months before 14 September 2019 or at least six months before the target date of the market of the dedicated interface. In practice, this means that ASPSPs should publish details of exactly which version/versions of each component are supported by their dedicated interface.
- As per RTS Article 30(4), ASPSPs must give TPPs at least three months' notice of any change to the technical specifications. In practice, this means that ASPSPs must give such notice if they are planning to introduce any updates to any component of the Standard, regardless of whether these are major, minor or patch updates. Any change may be implemented in an emergency situation (e.g. in the case where there is a security issue) without such notice, and in such situations ASPSPs must document emergency situations where changes are implemented and make the documentation available to competent authorities on request.
- As per RTS Article 30(5), ASPSPs must also make available a testing facility least six months before 14 September 2019 or at least six months before the target date of the market launch of the dedicated interface. As per the Final EBA Guidelines (Consultation Feedback Ref 119), ASPSPs should ensure that any changes are made available in the testing facility as soon as possible to allow TPPs to test against the updated technical specifications, in the context of compliance with Article 30(5). In practice, this means that ASPSPs should consider the impact of proposed changes on their testing facility in order to ensure that the testing facility enables the same functionality as the dedicated interface, in the context of such changes. As such, ASPSPs should endeavour to make any changes to the testing facility available to TPPs at least three months before changes are implemented to ensure TPPs, can continue to effectively test.
- ASPSPs should maintain multiple live/active versions of each interface (e.g. one for each supported release).
- Where an ASPSP choses to implement a new version of any component of the Standard they should implement each new major version within six months, and each new minor version within three months of the Standard being published by OBIE.

Together with the requirements for ASPSPs to notify TPPs of any changes (see section 5.5) any TPP will, except in an emergency, always have at least three months' notice before being required to update their systems.

5.2 Implementation of a new OBIE Standard

5.2.3 Considerations

5.2.3.1 Dual running and deprecation

ASPSPs should support a minimum of two API versions in a production context, providing both versions were previously supported by the ASPSP, for a period of time long enough to ensure that TPPs have had sufficient time to successfully test the new version and migrate their applications and customers. Where an ASPSP is using OBIE's Managed Rollout process, OBIE will be able to confirm when sufficient TPPs have migrated from the previous version to enable the ASPSP to reasonably demonstrate 'wide usage' of this new version. For all other ASPSPs, OBIE recommends dual running for at least six months for a major version, and three months for a minor version. Where an ASPSP implements an API for the first time, they will only need to support this one version to start with.

The ability to support two API versions allows TPPs to maintain existing integrations with the older version, and benefit from features and enhancements offered by the new version. Over time, TPPs will migrate all their applications to consume the new API version. Once migrated, TPPs should not access resources via the old API version (including creating, reading, updating or deleting).

Dual running of APIs requires a pragmatic approach to ensure that ASPSPs expose and support both API versions and to ensure that TPPs use these to migrate applications as intended, without unnecessary conflict.

The deprecation of unsupported versions is at the ASPSP's discretion - based on usage metrics. However, the OBIE may recommend that any specified version (major, minor, or patch) should be deprecated at any time, and this should be implemented within three months of notification by the OBIE. This is to cater for critical defects, especially those relating to security. In exceptional circumstances it may be agreed by OBIE that support for a specified version is terminated earlier.

ASPSPs must not apply any measures to induce TPPs to adopt a new version of the APIs (e.g. rate limiting the older version while providing better performance on a newer version).

5.2.3.2 API credentials, consent and authorisation

API Credentials associated to an API should be version agnostic. Therefore, a TPP accessing v1.0, v1.1 or v2.0 should be able to use the same API Credentials across all available API endpoints.

It in the domain of the TPPs to manage PSUs consent and ASPSPs to manage PSU authentication in compliance with relevant regulations.

If there is a non-breaking change (e.g. an additional field is added to a permission/cluster) then this should be managed between the TPP and PSU and between the ASPSP and PSU respectively. Any long lived access or refresh tokens could then remain unaffected.

In the event of a breaking change (e.g. where a permission/cluster is added, removed or changed), then the PSU may be required to re-consent with the TPP and to re-authenticate with the ASPSP.

5.2.3.3 Backward and Forward Compatibility

The OBIE specifications will include details on which operations or resources are expected to be backward and forward compatible across versions. It is expected that:

- A long-lived consent (e.g. for access to AISP resources) created using an older version of the APIs can be used for read operations in newer versions of the API.
- A short-lived consent (e.g. for a short lived payment initiation request) can only be used within the same version of the API for creating resources.

If an ASPSP is planning to release a new API version that does not follow the expectations above (e.g. does not support forward compatibility for AISP resources) this should be communicated to TPPs (e.g. via the OBIE's ASPSP Calendar).

5.3 Changes to an ASPSP's infrastructure, configuration or software

At any time, an ASPSP may need to make changes to any element of their system, including implementation of a new version (as described above). This includes the adding/removing of functionality or fields within an existing version. This may or may not require downtime.

In such cases, TPPs may need to update and re-onboard their application, and then re-test it in order to continue offering services via the ASPSP. This could result in increased costs, reduced revenue, and potentially customer loss, since services that PSUs rely on may be interrupted without prior warning.

For example, if the ASPSP has implemented a new authorisation server, TPPs will need to ask their PSUs to re-authenticate with the ASPSPs. PSUs could lose service entirely if there is any delay in a TPP re-connecting to the ASPSP. PSUs may have to re-authenticate to renew long lived consent (e.g. for the TPP to continue to access the PSU's data).

Where ASPSPs make such changes they should:

- Give TPPs a minimum of three months' notice of any such change, unless this is an emergency situation (Article 30(4) RTS).
- Document emergency situations where changes were made and make the documentation available to their NCA.
- To facilitate this, ASPSPs should report all changes to OBIE that could require TPPs to update/edit their code, where notice of any change will be added to the central noticeboard for the ecosystem.
- Re-run all relevant conformance tools.

5.4 Notification of a change

ASPSPs should provide notice to TPPs of a change (within the time frames outlined above) via the ASPSP's own website or developer portal.

When informing TPPs of an anticipated change, an ASPSP should confirm:

- Date notice is given
- Details of the change that will be made (e.g. implementation of new version)
- Reason for the change (e.g. new version to be implemented, old version to be deprecated, etc)
- Details of ASPSP system(s) affected (e.g. test facility, production interface)
- Details of how any change will be made available in the test facility in advance of the production interface
- Indication of the likely impact for a TPP, including any action required by TPPs (e.g. requiring PSUs to re-authenticate)
- Rating of the impact on the TPPs service:

Business critical issue - Business critical issue - represents a complete loss of service or a significant feature that is completely unavailable, and no workaround exists.

Degraded service issue - Degraded service issue - includes intermittent issues and reduced quality of service. A workaround may be available .

General issue – cosmetic issues which include product questions, feature requests and development issues in staging environments.

- Start time/date the change is anticipated to take effect and the end date/time (if applicable).

OBIE Support Services offers support to ASPSPs and TPPs, via the central noticeboard tool which publishes all notifications of change received from ASPSPs to the Open Banking ecosystem.

6.0 The Operational Guidelines Checklist

The Operational Guidelines Checklist (the OG Checklist) will serve as an essential tool that will enable Participants to self-attest against key criteria identified within the Operational Guidelines. Participants can answer specific questions to demonstrate conformance to the Operational Guidelines.

The FCA's own Checklist along with guidance in Chapter 17 of the PSRs Approach, as well as the EBA Guidelines, detail the regulatory requirements. We have developed the OG Checklist by placing OBIE recommendations underneath the FCA Checklist requirements.

We believe that successfully meeting all requirements and recommendations will support and facilitate an application for an exemption from the contingency mechanism. However, a UK-based ASPSP could choose to submit the FCA Checklist directly without reference to the OG Checklist and still gain an exemption.

ASPSPs applying for an Open Banking Operational Guidelines Conformance Certificate must submit a completed OG Checklist for each dedicated interface and each brand and segment. We note that multiple brands may have the same implementations and dedicated interfaces, which means the same OG Checklist can be submitted for each of them. Further, we encourage those completing the OG Checklist to consider if any additional submissions may be required e.g. if an ASPSP has "app-only" customers whereby having a consolidated OG Checklist could lead to different answers being provided for different customers.

For each OG Checklist submission, the business owner of the relevant brand/product should sign off and attest to its accuracy.

In developing the Checklist questions, we have defined some key principles that each question must adhere to:

- **OBJECTIVE** – be fact based and not rely upon the judgement of the ASPSP or TPP - quantitative evidence should be used wherever possible.
- **CLEAR** – standalone, single clause, closed questions which demand a “yes or no” answer.
- **DEFINED** – unambiguous and tightly constructed with links to definitions where appropriate.
- **TRACEABLE** based on regulatory requirements and/or the OBIE Standard (rationale for inclusion and classification will be made explicit).

6.1 The Operational Guidelines Checklist

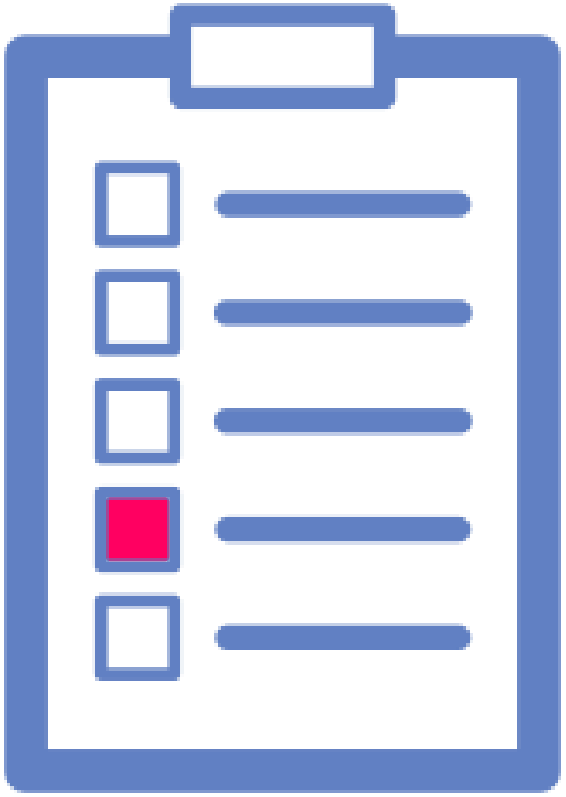
Under OBIE Requirements, the following terms are used:

- **Required** - participants must provide a response stated in column 'OBIE notes' in order to confirm conformance[1]
- **Recommended** - participants can self-attest conformance without implementing these items, however they are strongly encouraged to implement them in order to enable the desired ecosystem outcomes as described in the Operational Guidelines

There are some items marked as "Recommended" but that have been marked as mandatory under the CMA Order and are therefore required for the CMA9 for PCA/BCA.

The FCA Questions marked in bold and blue relate to the FCA's Questionnaire in their PS RTS Approach (pp. 52-57)

Operational Guidelines Checklist v1.1



[1]The notes provided by OBIE are intended to be helpful guidance on how an ASPSP could respond to the question but are not required. Further, OBIE will not issue an OG Conformance Certificate unless a participant has received an exemption from their NCA and self-attested against the desired responses stated in the 'OBIE notes' column.

OPEN BANKING