|  |
| --- |
| Data Integration Platform  DIP Subsidiary Document  DIP Assurance and Reporting  DSD003  Version 0.6  Date: DD Month YYYY |

DSD003 relating to reporting and Assurance in regards to the DIP.

1. Reference is made to the DIP Supplement of the Balancing and Settlement Code.

2. This is DIP Procedure DSD003, Version 0.4 relating to the reporting and Assurance requirements for DIP Users and the DIP Manager.

3. This DIP Procedure is effective from DD Month YYYY.

4. This DIP Procedure has been approved by the DIP Manager.

**Amendment Record**

| Version | Date | Description of Change | Approval Reference |
| --- | --- | --- | --- |
| 0.1 |  | Initial draft for Workgroup review | - |
| 0.2 |  | Second draft for Workgroup review | - |
| 0.3 |  | Issue 101 Consultation | - |
| 0.4 |  | Issue 101 Report | - |
| 0.5 |  | Shared with Ofgem |  |
| 0.6 |  | P474 |  |

**Contents**

[1 Introduction 5](#_Toc169521413)

[1.1 Scope and Purpose 5](#_Toc169521414)

[2 DIP Assurance 6](#_Toc169521415)

[2.1 DIP Assurance Risk Register 6](#_Toc169521416)

[2.2 DIP Assurance Strategy 6](#_Toc169521417)

[2.3 DIP User Assurance 8](#_Toc169521418)

[2.4 Assurance of DIP Service Provider 9](#_Toc169521419)

[2.5 Assurance of DIP Manager 9](#_Toc169521420)

[2.6 DCAB’s Assurance role 10](#_Toc169521421)

[3 Reporting 12](#_Toc169521422)

[3.1 DIP performance reports 12](#_Toc169521423)

[3.2 Sharing DIP Performance Reports 13](#_Toc169521424)

[3.3 Sharing of Message Contents 13](#_Toc169521425)

[4 Compliance and enforcement 14](#_Toc169521426)

[4.1 Compliance monitoring and reporting 14](#_Toc169521427)

[4.2 Compliance Stakeholder Engagement 15](#_Toc169521428)

# Introduction

## Scope and Purpose

The purpose of this DSD is to set out the arrangements for providing assurance that DIP Participants are adhering to the DIP Rules and processes.

The DIP has the capability to routinely produce Reports that will support the Authority, Code Bodies and other interested persons in meeting their need to gain assurance that DIP Users are adhering to their obligations under relevant industry arrangements. This DSD sets out how the DIP Manager may support such organisations by sharing information and providing reports relating to DIP Users’ use of the DIP.

# DIP Assurance

## DIP Assurance Risk Register

The DIP Manager shall maintain a DIP risk register of any potential matters that could lead a DIP Participant (or Participants), or the DIP, to be non-compliant with the DIP Rules (the “**DIP Risk Register**”). The DIP Risk Register shall contain a list of identified risks and for each risk shall provide:

1. risk descriptions, including who would be impacted if a risk was to occur;
2. probability, proximity, impact and risk assessments to create a risk score
3. the risk owner and details of any mitigating actions to be taken by the risk owner or other party
4. review dates based on current risk scores and proximity; and
5. the methodology to determine next review dates.

The DIP Manager shall review the Risk Register in its entirety at least quarterly; and shall brief the DCAB following each review; individual risks shall be reviewed on their due date.

Where new mitigations are identified following a review of the DIP Risk Register, the DIP Manager shall put in place an action plan to ensure the mitigation is given full effect. Where an action plan requires DIP Participant activity to mitigate the risk, such actions shall be agreed accordingly.

The DIP Risk Register and mitigation action plan(s) shall be published by the DIP Manager and updated following each review.

The DIP Manager shall issue guidance on how the Risk Register shall be compiled, shared and how stakeholders (including DIP Participants) may submit potential risks for inclusion.

## DIP Assurance Strategy

The DIP Manager shall determine and publish the DIP Assurance Strategy for the forthcoming DIP Year at least one month ahead of the start of each DIP Year. In determining the DIP Assurance Strategy, the DIP Manager shall consider:

1. the DIP Risk Register;
2. the quantity and nature of non-compliance incidents (including security breaches) over the previous DIP Year;
3. the potential for non-compliance in the forthcoming DIP Year based on:
   1. patterns of non-compliance;
   2. whether new rules due to be introduced could increase incidents of non-compliance;
   3. information received from Code Bodies, the Authority, or other interested persons;
   4. any other information the DIP Manager deems relevant;
4. the number of assurance analyses to be undertaken per DIP User type, and the type of analysis;
5. the number of audits per DIP User type and whether they will be site audits or desktop;
6. where the DIP Manager proposes to conduct audits, the minimum scope applicable to audits generally (additional scope can be added to specific audits);
7. any assurance activity to be carried out against DIP Manager that is due in the DIP Year for which the DIP Assurance Strategy will cover e.g. is the DIP Manager due their bi-annual external audit in the next DIP Year (in this context, the DIP Assurance Strategy shall reflect the DIP Manager’s internal assurance framework);
8. any assurance activity to be carried out against the DIP Service Provider that is due in the DIP Year for which the DIP Assurance Strategy will cover, and whether any service incidents over the previous year would lead to additional assurance activity;
9. any planned assurance activity in support of Code Bodies’ assurance of their respective Industry Code;
10. any planned assurance activity in support of the Authority or other interested persons;
11. the type, periodicity and content of DIP performance reports to be published;
12. assurance activity identified in DSD002 Annex 3 ‘The DIP-PKI (Public Key Infrastructure) Policy’ and reviews of said policy and associated processes; and
13. any other matters that the DIP Manager deems to be required to seek assurance that DIP Participants are complying with the DIP Rules and/or obligations under Industry Codes to which use of the DIP is a requirement.

Prior to finalising and publishing the DIP Assurance Strategy for the forthcoming year, the DIP Manager shall consult on their strategy for a period of at least 15 WD.

In determining their DIP Assurance Strategy, the DIP Manager shall, so far as practicable, ensure that any actions proposed will avoid replication of assurance activity undertaken by Code Bodies, the Authority or similar organisations where appropriate. This paragraph shall only have effect where Code Bodies, the Authority or similar organisations have agreed to share assurance activity findings, thus avoiding the need for replication.

To enable these efficiencies the DIP Manager shall ensure the views and suggestions of Code Bodies, the Authority and similar organisations are considered as part of the strategy consultation process. The DIP Manager should also consider where they are able to share the findings of any DIP assurance activity with Code Bodies, the Authority or similar organisations.

With respect to the Assurance priorities set out in the DIP Manager’s proposed Assurance Strategy, DCAB may suggest alternative and/or additional priorities as it thinks fit. Where DCAB makes such suggestions then the DIP Manager shall take those suggestions into account in adopting the DIP Assurance Strategy.

Except in the case of emergency or instruction by the Authority, wherever reasonably possible, the DIP Manager will endeavour to ensure that the conduct of any Assurance activities does not unreasonably disrupt DIP Participants and that, where possible, audits are co-ordinated with other Code Bodies in order to minimise disruption.

## DIP User Assurance

The DIP Manager shall analyse information within the reports created pursuant to this DSD to identify any potential non-compliance or areas of concern. The DIP Manager may make use of analytical software, or other appropriate methodologies to achieve this.

The DIP Manager may carry out audits of DIP Users to assure itself that the DIP User is acting in accordance with the DIP Rules. DIP User audits may be in accordance with the DIP Assurance Strategy, or for other purposes where deemed necessary by the DIP Manager.

Audits may be either on-site or remote ‘desktop’ audits, and may be carried out by third parties on behalf of the DIP Manager.

Where the DIP Manager intends to audit a DIP User, the DIP Manager shall (unless the circumstances require otherwise) inform the DIP User of its intention at least one month in advance.

Where the DIP Manager intends to audit a DIP User, the DIP User shall comply with any reasonable requirements made upon them by the DIP Manager. So far as practicable, the DIP Manager and DIP User shall endeavour to agree timings, locations etc. but, where agreement cannot be reached, the DIP Manager shall direct the DIP User to support the audit as required and the DIP User shall be expected to support the audit as directed by the DIP Manager.

DIP assurance reports shall be completed as soon as reasonably practicable on completion of assurance activity. Reports shall be shared with the DIP User and the DIP Manager shall, if required, agree a rectification plan with the DIP User. Rectification plans shall include, amongst other things, the activities to be undertaken and the associated completion dates. Where the DIP Manager and DIP User cannot agree a rectification plan, the DIP Manager shall direct the DIP User to rectify their short-comings as the DIP Manager believes appropriate, including within a timeframe dictated by the DIP Manager.

Where there is the opportunity for wider learning, the DIP Manager may consider publishing aspects of a DIP User’s report in accordance with DSD006 ‘DIP Data Management’.

DIP Users should endeavour to keep the DIP Manager appraised of any non-DIP assurance activity they are expecting to be subject to so the DIP Manager may take this into consideration when planning potential assurance activity.

## Assurance of DIP Service Provider

The DIP Manager shall ensure that its contract with the DIP Service Provider includes a requirement for the DIP Service Manager to provide to the DIP Manager access to:

1. the systems, system specifications and other systems documents used by the DIP Service Provider in connection with performing its obligations and functions as DIP Service Provider; and
2. its premises, personnel, data, information and records.

Access shall be sufficient to enable the DIP Manager to properly undertake its audit in accordance with the DIP Rules and the DIP Assurance Strategy.

Performance levels, and the DIP Service Provider’s performance against them shall be published by the DIP Manager subject to the requirements of DSD006 ‘DIP Data Management’ and any confidentiality conditions which might affect the DIP Manager. Where the DIP Service Provider’s agreement with the DIP Manager is subject to review, the DIP Manager shall seek the views of DIP Users and other key stakeholders as to the validity of previously agreed performance levels.

The DIP Manager shall audit the DIP Service Provider commensurate with the DIP Assurance Strategy (or at any other time should the DIP Manager deem necessary), and at least every two year; the findings of which shall be published subject to confidentiality constraints.

In determining the scope of any audit of the DIP Service Provider, the DIP Manager shall seek the views of the DCAB.

## Assurance of DIP Manager

The purpose of this section is to provide a framework for giving assurance to DIP Users that the DIP Manager is complying with the DIP Rules.

The DIP Manager shall maintain, or have access to, a sufficiently independent internal audit function to undertake the assurance described in this section.

The DIP Manager shall, in respect of the first DIP Year and once every two years thereafter, appoint a suitably independent external auditor to undertake an audit of the DIP Manager’s compliance with the DIP Rules.

Where the DIP Assurance Strategy calls for the DIP Manager to be audited, the scope of that audit shall be discussed with the DCAB prior to being finalised and the DCABs feedback shall be incorporated into the audit scope. Where there is disagreement between the DIP Manager and DCAB on the scope of the audit, the DCAB’s requirements shall prevail.

DIP Manager Audits shall be conducted pursuant to the DIP Assurance Strategy. As a minimum the DIP Manager shall ensure that its internal audit framework undertakes audits as follows:

1. at least annually (save that where an external audit is performed under paragraph 2.5.3 then this may replace the annual internal audit);
2. following a material DIP Change (see DSD004 ‘DIP Change and Document Management’);
3. where more than half of the DIP Manager’s personnel have changed since the last audit;
4. following the introduction of new obligations on the DIP Manager which will cause the DIP Manager to amend their business processes (if in doubt, the DCAB shall confirm where action is required).

The DIP Manager shall publish a summary statement of the findings of the DIP Manager Audit and, if applicable, the rectification plan which shall be updated monthly until all findings have been rectified.

## DCAB’s Assurance role

The DCAB shall review the DIP Assurance Strategy at the next normal DCAB meeting following publication and shall provide comment within the same timelines as other correspondents.

DCAB comments can be provided in writing or verbally to the DIP Manager’s representative at DCAB. Where verbal comments are provided, they shall be captured in DCAB meeting minutes.

The DIP Manager shall inform the DCAB each month of what assurance activity has been undertaken, specifically:

1. number of DIP User analyses undertaken per DIP User type;
2. number of Audits undertaken per DIP Participant type;
3. number of assurance rectifications complete;
4. number due in the next month;
5. any rectifications outstanding;
6. any lessons learned from assurance activity and/or incidents, and details of how they will be actioned;
7. any appeals raised against the DIP Manager in relation to DIP Assurance activity; and
8. any other matters that the DIP Manager considers relevant.

# Reporting

## DIP performance reports

The DIP will auto-generate the reports listed in this section on the fifth Calendar Day of each calendar month in respect of the previous calendar month. DIP Users will have access to these reports and real-time alerting via a dashboard. DIP Users will be able to configure their individual reporting and alerting requirements from the dashboard, e.g. via email.

The content of performance reports will be set by the DIP Manager in the DIP Assurance Strategy. Where the DIP Assurance Strategy changes the content/type etc. of performance reports from one DIP Year to the next, this shall be considered as a DIP Change and the DIP Manager shall act in accordance with DSD004 ‘DIP Change and Document Management’.

DIP messages have a number of key attributes (tags) available in the message header, which can be commonly linked across related message channels, such as a correlation ID, transaction ID and MPAN. These can be used to create reports that link business processes across the various channels and can provide an audit trail in close to real-time (50% of reports will be returned within 5 seconds, and 100% within 30 seconds).

Some examples of DIP performance reports may include:

1. number of MPANs per DIP Payee for funding purposes (see DSD005 ‘Funding and Budget’);
2. faults that have been detected and whether they have been rectified;
3. periods of unplanned down-time and time to rectify;
4. API Activity – requests, who, when, what;
5. number of messages held in dead-letter queue;
6. data latency – end-to-end transaction times between the time messages arrive via the incoming API call and the time the corresponding HTTP response code was sent;
7. volume of messages per message type (e.g. IF002) broken down multiple ways e.g. per DIP User or per DIP Role; and
8. anything further required by the DIP Manager.

Primary access to reports for DIP Users will be achieved through the DIP Portal. DIP Users will only be allowed to see reports for items they are authorised to view; for example, they will only view individual MPANs that they are responsible for.

Reports that do not show sensitive data, say for performance throughput where totals are reported, will not have this restriction.

## Sharing DIP Performance Reports

The DIP Manager may create and share reports (subject to the requirements of DSD006 ‘DIP Data Management’) regarding DIP Users’ use of the DIP with organisations such as (but not limited to):

1. Code Bodies;
2. auditors appointed by Code Bodies to undertake audits of Industry Codes;
3. the Authority;
4. government departments;
5. industry regulatory bodies; and
6. auditors appointed by the DIP Manager.

The nature and content description of specific reports shall be published by the DIP Manager and shall include reports relating to the processes in Industry Codes that require the use of the DIP.

Any person may request copies of reports created under this DSD pursuant to the requirements of chapter 7 ‘Information Security and Data Management’ of the DIP Supplement and DSD006 ‘DIP Data Management’.

## Sharing of Message Contents

The DIP Manager shall not disclose the content of any Message between DIP Participants unless the requester:

1. is the Authority and they are requesting the content of a Message;
2. has shown there is a legitimate regulatory need to see the contents of a Message;
3. has demonstrated that the controls the requester will place around the data are equivalent to or better than the DIP Manager’s data controls; or
4. is willing to be audited by the DIP Manager (or their representative) to ensure the data has been treated as per sub-paragraph c of this paragraph.

Any requests for the DIP Manager to report on the content of any Message sent via the DIP shall be subject to Data Management triage and mitigation processes set out in DSD0006 ‘DIP Information Security and Data Management’.

# Compliance and enforcement

## Compliance monitoring and reporting

The DIP Manager shall monitor DIP Participants’ compliance, including making a record of non-compliance.

Subject to the data triage and mitigation principles specified in chapter 7 ‘Information Security and Data Management’ of the DIP Supplement and DSD006 ‘DIP Data Management’, the DIP Manager may publish a list of non-compliance incidents by each DIP User.

Where the DIP Manager becomes aware of non-compliance with the DIP Rules by a DIP Participant, the DIP Manager shall inform the relevant Code Bodies to which the DIP User is party. The DIP Manager shall continue to liaise with the Code Bodies to determine which Code Body or Code Bodies shall take the case forward and whether further information is required from the DIP Manager.

Where the DIP Manager identifies any material or substantial non-compliance with obligations of a DIP Participant that they think requires further action beyond those listed in this DSD, the DIP Manager may engage with the Authority to determine the most appropriate way to proceed.

Where the DIP Manager engages with the Authority to pursue potential enforcement action, each case shall be treated as the circumstances and situations of the case may require.

The DIP Manager shall work with Code Bodies, the Authority and other such bodies to identify commonalities in non-compliance and synergies in addressing non-compliance where applicable.

At least annually the DIP Manager shall publish a report covering:

1. the number of incidents of non-compliance and any actions taken;
2. the names of non-compliant DIP Users;
3. details of audits undertaken and themes in findings (including DIP Manager and DIP Service Provider if applicable);
4. any themes identified through report analysis;
5. the number and details of service incidents effecting DIP availability and/or integrity;
6. where the DIP Manager was unable to achieve the DIP Assurance Strategy; and
7. anything else relating to DIP Assurance.

## Compliance Stakeholder Engagement

The DIP Manager shall publish newsletters at least quarterly with details of planned DIP Changes, audit priorities and assurance focus for the forthcoming quarter.

The DIP Manager shall host stakeholder engagement workshops to discuss DIP best practice, assurance focus and compliance concerns at least twice per year.

The frequency of stakeholder engagement, and types of engagement may be increased at the DIP Manager’s discretion as they deem necessary and/or as required by the DIP Assurance Strategy.