Pensions Dashboards Programme

Reporting standards

July 2022

pensionsdashboardsprogramme.org.uk

Money & Pensions Service

Contents

1. Introduction

About the standards

The reporting standards ensure that pension schemes (both occupational as well as stakeholder and personal pension schemes connected to the pensions dashboards ecosystem) (pension providers) and qualifying pensions dashboard services (QPDS) understand what information is required to be generated by them and provided to Pensions Dashboard Programme (PDP) (on behalf of Money and Pensions Service (MaPS)) for reporting purposes. It also supports monitoring the effectiveness and overall health of the central digital architecture (CDA) and the pensions dashboard ecosystem.

The standard ensures there is consistency across both data providers and QPDS. When we refer to data providers in this standard this covers pension providers and their third parties. Third parties, such as administrators or software providers, will in practice apply these standards and guidance on behalf of their clients. We expect that much of the implementation of this standard will be undertaken by such third parties on behalf of multiple clients. This will mean in practice that for a pension provider (or QPDS) connecting via an already-connected third party, much of these security, service, connection, and operational standards will already have been met prior by the third party on the pension provider's (or QPDS') behalf to that pension provider's connection being turned on via that existing connection. However, as the standard applies to the pension provider (or QPDS), the pension provider (QPDS) is responsible for compliance with them, even if they delegate the implementation of the standards to a contracted third party.

The standard also outlines the data required to support oversight by Financial Conduct Authority (FCA), the Pensions Regulator (TPR), Department of Work and Pensions (DWP) and PDP (on behalf of MaPS). Detailing the data pension schemes and QPDS need to produce support the monitoring and enforcement of compliance with duties and inform on continuous improvements.

Reporting standards are separate from, but designed to complement, the FCA's regulatory framework. As the FCA regulates the conduct of firms carrying out an activity, the FCA's Handbook rules will apply to QPDS firms and can impose standards on those firms (aligned to FCA's statutory objectives) when carrying out the qualifying pensions dashboard service. The FCA will consult on its proposed Handbook rules in due course.

2. Scope

For pension providers and QPDS to provide data on a regular basis that will be used alongside data generated within the ecosystem, in order to provide the following:

- **audit information**
    - **business audit** - information required for non-repudiation purposes, and / or to help us understand what has happened when something goes wrong at the individual user level
- **ecosystem monitoring information**

    - **protective monitoring** - information including transaction monitoring, (sometimes referred to as 'cyber' monitoring) for security protection and detection
    - **operational monitoring** - information for the purposes of the operational management centre to operate the system and measure its performance in technical terms
- **ecosystem insight**
    - **management information** - information (including operational, financial, and performance data) that allows us to assess how dashboards QPDS are being used and whether they are delivering the required service their goals, including operational, financial, and performance data defined by internal and external stakeholders
    - **oversight reporting** - information that will allow regulators, PDP and other oversight bodies to determine whether PDP, individual data providers (pension schemes plus any administrators or integrated service providers carrying out their dashboard functions), and/or individual QPDSs QPDS are meeting their obligations. This will allow regulators, for instance, to take action against pensions schemes that are failing to meet their obligations.

These types of logging may overlap in terms of data items involved and potentially in purpose across the categories, but it is hoped that the classification is helpful background.

3. Summary

The following table provides a summarised list of the data feeds that will be required from data providers and QPDSs:

Source	Event	Satisfies	Frequency
QPDS	Authentication to CDA	Business audit	High – each time a user re-directs to C&A
QPDS	Dashboard redirects to C&A	Business audit Protective Monitoring	High – each time a user re-directs to C&A
Data Provider	PEI create, update, delete (CRUD)	Business Audit Protective Monitoring	High – every significant CRUD event
Data Provider	View Response	Business Audit Protective Monitoring	High – every view response
QPDS	Indicators of security compromise	Protective Monitoring	Near real time
QPDS	Connection handshake errors	Protective Monitoring	Near real time
Data provider	Indicators of security compromise	Protective Monitoring	Near real time
Data Provider	Connection handshake errors	Protective Monitoring	Near real time
QPDS	Operational status of the QPDS	Operational Monitoring	High - Every 10m per QPDS
Data Provider	Data Provider End Point Monitoring	Operational Monitoring	High - Every 15s per Data Provider
QPDS	Report – view requests from dashboard	MI Reporting	Low – Daily
QPDS	Report – logins from dashboard	MI Reporting	Low – Daily
QPDS	Report – Acknowledgements from View request	MI Reporting	Low – Daily
QPDS	Report – Dashboard dropout statistics (needs more definition)	MI Reporting	Low – Daily
Data Provider	Re-finds	MI Reporting	Low – Daily

Data Provider	Found but not viewed	MI Reporting	Low – Daily
QPDS	Complaints	Oversight reporting	Low – Daily
QPDS	Unsuccessful views	Oversight reporting	Low – Daily
QPDS	Pension owner usage	Oversight reporting	Low – Daily
QPDS	SLA adherence	Oversight reporting	Low – Daily
QPDS	Uptime	Oversight reporting	Low – Daily
Data provider	Complaints	Oversight reporting	Low – Daily
Data provider	View statistics	Oversight reporting	Low – Daily
Data provider	PEI registration SLA	Oversight reporting	Low – Daily
Data provider	Uptime	Oversight reporting	Low – Daily

4. Reporting standards

4.1 Business audit

A business audit event is the recording of an event of significance. Its primary purpose is to ensure the creation of records which assist in the non-repudiation of those events. This enables proof of users' actions and the causal relationships between users when events take place.

Business audit events are those which:

- release data from one domain to another and must be recorded
- lead to the persistence of data, or its modification
- enable control of, or dependency, between events across domains

External users, the human users are *pension owners and their delegates*, the system users are the CDA, dashboards, data providers, and identity services.

For data providers and QPDS the events that they must provide for business audit are detailed in the sections below.

General (applies to data providers and QPDS)

Business audit events are by definition at the level of individual user activity: they enable investigation and non-repudiation of each significant action taken by the user and the system components which act for the user.

General data items for business audit

Both QPDS and data providers must provide the following data items

Data Item	Description	Comment
Event type	**Alphanumeric** code used to identify the event	i.e. DAPA001 where 'DAP' – Data Provider, 'A' – Audit, '001' – numerical identifier for event type
Request_id	A GUID generated by the party which initiates any transaction in the ecosystem and is to be stored in the audit log of the initiator and recipient Standards for the Request_id generation are detailed in the technical standards	Request_id will be a parameter of a business transaction API *and* it will be included in all related audit or monitoring calls

Data Item	Description	Comment
Date time stamp	Date+time of the event	Applies to all audit, monitoring or reporting events

Also, both QPDS and data providers should be ready to provide mediated access to their internal audit records. In the event of investigation of a customer complaint or security incident, or any activity requiring regulatory (or other) investigation. These internal audit records should also contain any unique transaction identifiers supplied to, or received from, the CDA, to ensure no individual user's details are disclosed (the standard for these transaction identifiers can be found in the technical standards).

QPDS business events

QPDS must create business event data and send to the CDA when:

- their infrastructure authenticates to the CDA
- for each user who is redirected to the CDA (for whatever reason)

QPDS Data Items

Data Item - What specific data QPDS must provide	**Description**	**Comment**
Client_auth	OAuth client authentication status	Audit success or failure (and reason code) for Dashboard to C&A client authentication
Redirect	Reason for redirect to CDA	Separately audited to provide a separate record of intent in addition to the via the user agent transaction See also Authentication Context in Protective Monitoring

Data providers

Data providers must create business event data and send to the CDA when:

- the data provider creates/updates/deletes a registration of the Pensions Identifier (PeI), and the reason.
- the data provider responds to a view request

Data provider data items

Data Item - What specific data data providers must provide	**Description**	**Comment**
View_request_id	The request_id which the data provider received from the dashboard which initiated the view transaction	Audited at CDA to provide a central non-repudiatable record that a data provider released a pension details payload to a dashboard The data provider will also audit this event in its internal audit log, including the relevant request_id

PeI registration (CRUD) are **business transactions** which will be audited at CDA.

Data Item	**Description**	**Comment**
Registration_reason	Match-yes, match-maybe, match-no, match-withdrawn, asset-removed	Various reasons for PeI registration for reasons of normal & maybe matching, deleting matched and moving/transferring assets
Find_request_id	The request_id of the inbound find which initiated this registration event	Or null if this is a transfer/error correction transaction

Frequency

Business audit events must be generated immediately by data providers and QPDS after the original business transaction has been processed. These records must be sent in near real time (NRT) to the CDA but at least within an hour of the event taking place by data providers and QPDS.

Audit interface

API to be exposed through the CDA architecture API gateway

- call using Https / Json.

The view request interface must contain the request id generated by the QPDS.

4.2 Protective monitoring

Protective monitoring, transaction monitoring, 'cyber' monitoring, enable prevention or detection of incidents which relate to the secure operation of the service.

This helps the CDA to identify attack indicators, and looks for indicators of compromise, detecting events and raising incidents to be handled by the CDA's security operations centre (SOC).

General data items for protective monitoring

Both QPDS and data providers must provide the following data items

Data Item	Description	Comment
Event type	Alphanumeric code used to identify the event	i.e. DASP001 where 'DAP' – QPDS, 'P' – protective monitoring, '001' – numerical identifier for event type
Request_id	A GUID generated by the party which initiates any transaction in the ecosystem and is to be stored in the audit log of the initiator and recipient Standards for the Request_id generation are detailed in the technical standards	Request_id will be a parameter of a business transaction API *and* it will be included in all related audit or monitoring calls
Date time stamp	Date+time of the event	Applies to all audit, monitoring or reporting events

QPDS protective monitoring event

QPDS must generate a protective monitoring event feed to CDA when:

- data (eg IP address, user agent fingerprint, local authentication event – authentication type, failed tries, last successful login, indicators of compromise (IoC)) when the user is redirected to the CDA).
- connection/handshake failures with (data provider) View end points (MTLS, cypher suite, protocol related failures)
- connection/handshake failures with CDA (MTLS, cypher suite, protocol related failures)

As part of their overall dashboard co-operation duty, QPDS shall contribute intelligence relating to ecosystem security to the PDP security operating centre (SOC) and receive and act appropriately on intelligence received from the SOC.

QPDS protective monitoring data items

What specific data QPDS must provide

Data Item	Description	Comment
Source IP	The source IP of the request to access the dashboard before redirection to CDA.	Enables cross organisational monitoring of the user agent and its potential interception/MiTM attacks.
Location	Conditional Access location (Access from the UK)	
Additional information	Free text message E.g., Poor TLS attempt TLS 1.0	Monitoring connection handshakes
ID_service	Package of information related to the use of pension owner or delegate identity services	May be required if the QPDS choses to use the ecosystem identity providers at the dashboard

Data provider protective monitoring event

Data providers must generate a protective monitoring to be sent to the CDA when:

- data (e.g. IP address, IoC) when a dashboard connects/calls a view endpoint (e.g. failure of bound tokens, presentation of invalid data values/tokens)
- connection / handshake failures with (dashboard) end points (MTLS, cypher suite, protocol related failures)
- connection / handshake failures with CDA (MTLS, cypher suite, protocol related failures)

As part of their overall dashboard co-operation duty, data providers shall contribute intelligence relating to ecosystem security to the PDP SOC and receive and act appropriately on intelligence received from the SOC.

Data provider protective monitoring data items

What specific data, data providers must provide

Data Item	Description	Comment
Dashboard_IOC	Package of information related to misbehaving/error modes of the protocol from dashboards to data providers	Data provider monitors behaviour of dashboards when not operating normally
Additional information	Free text message describing the event E.g., Poor TLS attempt TLS 1.0	Monitoring connection handshakes

In addition to the above, providers will also exchange soft reports by secure channels related to ecosystem security intelligence to support the pan ecosystem SOC.

Frequency

Protective monitoring events must be generated immediately after a security event is established. These records must be sent in NRT to the CDA but at least within an hour of the event taking place by data providers and QPDS.

Protective monitoring interface

API to be exposed through the central digital architecture API gateway

- call using Https/Json.

4.3 Operational monitoring

Operational monitoring provides metrics and alerts, which enable the reliable operation and management of the service as a whole by the CDA's operational management centre.

Operational Monitoring provides metrics which enable the reliable operation of, and coordination thereof, the service as a whole by the CDA's Operational Management Centre.

General data items for operational monitoring

Both QPDS and data providers must provide the following data items

Data Item	Description	Comment
Event type	Alphanumeric code used to identify the event	i.e. DASO001 where 'DAS' – QPDS, 'O' – protective monitoring, '001' – numerical identifier for event type
Date time stamp	Date+time of the event	Applies to all audit, monitoring or reporting events

QPDS operational monitoring event

A QPDS must contribute operational monitoring to CDA when:

- operational status of the dashboard service/infrastructure
- lost user volumetrics – the number of redirects to CDA for which a user does not return in accord with PDP protocols in a time period. (Period has to be much larger than the expected time at the CDA e.g. 30mins.)

QPDS operational monitoring data items

What specific data a QPDS must provide

Data Item	Description	Comment
Operational_Status	Package of information related to the operational status of the dashboard service	Enables reporting of service characteristics centrally and potentially management of complaints/enquiries related to other parts of the ecosystem
User_Lost_at_CDA	Number of users (and % of overall users) per time period who did not return to the dashboard after they were redirected to CDA	This item is related to similar reporting items, but is here to enable a faster response if operational failures indicate issues

Data provider operational monitoring event

Data providers must contribute operational monitoring to CDA when:

- operational status of each endpoint (find or view) eg every 15 secs report endpoint URL, up/down, load/capacity
- operational status of all the Find and View endpoints managed by the data provider, to include up/down and average response time over the period. (Period may be set following consultation, eg average over 2 mins.)

Data provider operational monitoring data items

What specific data, data providers must provide

Data Item	Description	Comment
Operational_Status	Package of information related to the operational status of the data provider find and view endpoints. Frequent monitoring – at least every 15 secs	Enables management of operational status of ecosystem and proactive management of failures at data providers

Data Item	Description	Comment
Scheme	URL of endpoint and list of the schemes (holdernames) which are within the scope of the endpoint, including availability and average & max response times over a short time window such as 2 mins	CDA only 'sees' Find Endpoints and QPDS only see View endpoints. Neither type of endpoint is necessarily operational in respect of the schemes which it serves (typically and endpoint will serve data related to many schemes). Accordingly, this monitoring interface enables providers to understand if the scheme is attached to the end point

Frequency

Operational monitoring events must be provided by QPDS every 10 mins and data providers every 15 seconds.

Operational monitoring interface

API to be exposed through the central digital architecture API gateway call:

- using Https/Json

4.4 Management information

Information (including operational, financial, and performance data) that allows us to assess how QPDS are being used and whether they are delivering the required service.

QPDS management information required

A QPDS must contribute management information to CDA for:

- Number of view requests initiated from a dashboard
- Number of times QPDS have been logged into
- Number of times QPDS used by Guest (i.e not logged into)
- Numbers of acknowledgements received back from a view request
- Number of times a user journey is not completed (drop off rate)

QPDS management information data items

What specific data a QPDS must provide

Data element	Description	Comment
Source	The name (or id) of the source QPDS	
Event type	Code identifying the type of event (exact code(s) to be defined)	E.g. DASA001. 'DAS' – Dashboard, 'M' – Management Information, '001' – numerical identifier for event type
Metric	Metric associated with the event	
Report Start date	Start date of reporting period	
Report End date	End date of reporting period	Based on daily reporting, the end of the reporting period will be the same as the end date of the reporting period. However, this interface design will allow the length of reporting periods to change in the future
Date time stamp	Date and time the activity took place	

As part of their overall dashboard co-operation duty, QPDS shall make available to PDP data they collect from their own surveys regarding the pensions dashboard service.

Data provider management information required

A data provider must contribute management information to CDA for:

- Average number of re-finds of the same asset within a period (month, quarter, year) per pension provider
- Number of assets found but not viewed within a period (month, quarter, year) per pension provider

Data provider management information data items

What specific data a data provider must provide

Data element	Description	
Source	The name (or id) of the source data provider	
Event type	Code identifying the type of event (exact code(s) to be defined	E.g. DASA001. 'DAS' – Dashboard, 'M' – Management Information, '001' – numerical identifier for event type
Pension provider	Repeating structure for each provider	
Time Period	Code representing time period	month, quarter, year
Metric	Metric associated with the event	
Report Start date	Start date of reporting period	
Report End date	End date of reporting period	Based on daily reporting, the end of the reporting period will be the same as the end date of the reporting period. However, this interface design will allow the length of reporting periods to change in the future
Date time stamp	Date and time the activity took place	

Frequency

Management data will be summarised in on a daily basis as opposed to sending individual events.

Management information interface

API to be exposed through the central digital architecture API gateway call:

- using Https/Json

4.5 Oversight

Oversight reporting is to enable an oversight body (FCA, TPR, DWP) to manage compliance and non-compliance of regulated entities and PDP to have oversight of participants behaviour. Note that CDA provides an effective conduit for data and for its appropriate association and standardisation in reports.

QPDS oversight information required

A QPDS must contribute oversight information to CDA for:

- number and nature of complaints raised to the QPDS by an individual related to pensions dashboards
- number and nature of complaints being processed (excluding those raised in the time period) to the QPDS by an individual related to pensions dashboards
- individual unsuccessful view requests and reason (including where no value data is returned)
- average (mean, median & mode) number of times an individual uses a dashboard
- average view response times within SLA in line with code of connection
- individual view responses outside SLA in line with code of connection
- uptime over time for each QPDS within a period (month, quarter, year)

Also, both QPDS and data providers should be ready to provide access to detailed complaints information related to pensions dashboards.

QPDS oversight data items

What specific data a QPDS must provide

Data element	Description	Comment
Source	The name (or id) of the QPDS	
Event type	Code identifying the type of event (exact code(s) to be agreed).	E.g. DASA001. 'DAS' – Dashboard, 'O' – Oversight, '001' – numerical identifier for event type
Metric	Metric associated with the event	
Time Period	Code representing time period for mode average	month, quarter, year

Request ID	A GUID generated by the party which initiates any transaction in the ecosystem. This is used when reporting individual events	
Reason	If applicable the reason for an event	Likely to be a predefined list of reasons
Report Start date	Start date of reporting period	
Report End date	End date of reporting period	Based on daily reporting, the end of the reporting period will be the same as the end date of the reporting period. However, this interface design will allow the length of reporting periods to change in the future
Date time stamp	Date and time the activity took place	

Data provider oversight information required

A data provider must contribute oversight information to CDA for:

- number and nature of complaints raised to the data provider or pension provider by an individual related to pensions dashboards
- number and nature of complaints being processed (excluding those raised in the time period) to the data provider or pension provider by an individual related to pensions dashboards
- individual unsuccessful view requests and reason (where a PeI has been registered but where when requested to return data the pension provider was unable to or could not provide value information)
- total number of view requests per pension provider
- average time to register a PEI within SLA in line with code of connection
- individual events to register a PEI outside SLA in line with code of connection
- uptime over time for each data provider within a period (month, quarter, year)
- uptime over time for each pension provider within a period (month, quarter, year)

Data provider oversight data items

What specific data a data provider must provide

Data element	Description	

Source	The name (or id) of the Data Provider	
Pension Provider	Id of pension provider	
Event type	Code identifying the type of event (exact code(s) to be agreed).	E.g. DASA001. 'DAS' – Dashboard, 'O' – Oversight, '001' – numerical identifier for event type
Metric	Metric associated with the event	
Time Period	Code representing time period	month, quarter, year
Request ID	A GUID generated by the party which initiates any transaction in the ecosystem. This is used when reporting individual events	
Reason	If applicable the reason for an event	Likely to be a predefined set of reasons
Report Start date	Start date of reporting period	
Report End date	End date of reporting period Based on daily reporting, the end of the reporting period will be the same as the end date of the reporting period. However, this interface design will allow the length of reporting periods to change in the future	
Date time stamp	Date and time the activity took place	

Frequency

Reporting events must be provided on a daily basis by a data provider or QPDS.

Oversight information interface

API to be exposed through the central digital architecture API gateway call:

- using Https/Json