

Code of connection

The code of connection sets out how pensions providers and schemes, and dashboards providers are to connect to the dashboards ecosystem and what they need to do to remain connected. It details the mandatory requirements that must be met, as well as the recommended ways in which participants should implement them.

The code of connection will combine the required security and operational standards, which ecosystem participants will have to adhere to. It will provide a standard of expected behaviour to protect all ecosystem participants.

Draft version 1.1

All PDP standards are published as 'draft' until approved by the Secretary of State for Work and Pensions. Find out more about PDP's [approach to standards governance](#).

PDP recommends schemes and providers align with the current version whilst preparing for connection. This version was developed following industry consultation and review by PDP volunteer participants.

PDP may make further changes before seeking formal approval. Only necessary changes will be considered and we will work with industry to understand potential impacts

Refer to the [changelog](#) for updates since the last publication.

Introduction

Summary

1. Pensions dashboards are apps, websites or other tools which help individuals view information about their multiple pensions in one secure place online, at a time of their choosing. They bring together information on all a user's (in-scope) pensions, including their State Pension, as well as any occupational and personal pensions. This supports individuals' engagement with their pensions and their planning for retirement.
2. The Money and Pensions Service (MaPS) set up the Pensions Dashboards Programme (PDP) in 2019 to design and build the central digital architecture (CDA) and services that make pensions dashboards possible. PDP are also responsible for the supporting governance framework, service design and operating model for the pensions dashboards ecosystem.
3. The pensions dashboards ecosystem enables millions of individuals to connect with their pensions information through multiple dashboards across thousands of pension providers and schemes. Find out more about the [pensions dashboards ecosystem and its components](#).

4. MaPS is responsible for operating its own non-commercial, pensions dashboard as a public service.

Purpose

5. This code of connection is issued by MaPS under delegated powers given by the Pensions Dashboards Regulations 2022 and the Pensions Dashboards Regulations (Northern Ireland) 2023 (referred to hereafter as 'Regulations') and the Financial Conduct Authority (FCA) Pensions Schemes (Information to Dashboards) Instrument 2022/38 rules for pension providers (hereafter 'Rules').

6. The code of connection comprises of the security, service, and operational standards. These standards set out the requirements that must be met to connect to the pensions dashboards ecosystem and the requirements that must be met to remain connected.

7. The code of connection provides assurance that the systems and services of all participants in the ecosystem, which access and use the central digital architecture and interoperate with other ecosystem participants, are managed and controlled to the appropriate levels.

8. Together, these will ensure that the pensions dashboards ecosystem provides a secure, well-functioning, effective service which garners user trust and satisfaction, which facilitates pension providers to comply with their legal duties, and enables multiple dashboards to operate, creating choice for users and scope for innovation.

9. The code of connection comprises 3 sets of standards:

Security standards

- **Description:** The ongoing technical and procedural standards required to ensure the appropriate level of security for the pensions dashboards ecosystem.
- **Purpose:** To deliver a secure service in which users, pension providers and dashboards can all have trust.

Service standards

- **Description:** The minimum service requirements and required behaviour of participants.
- **Purpose:** To deliver an effective, well-functioning and high performing service that ensures all participants operate to the same level and know what to expect from each other, and that ensures users have a positive user experience.

Operational standards

- **Description:** The minimum operational processes participants must follow to maintain their connection into the ecosystem.
- **Purpose:** To ensure effective ongoing operation of the ecosystem.

Audience

10. These standards apply legally to the trustees or managers of occupational pension schemes (pension schemes), the managers of stakeholder and personal pension schemes (pension providers), and to qualifying pensions dashboard services connected to, or required to connect to, the pensions dashboards ecosystem.

11. Where pension providers and schemes or where pensions dashboard services connect to the ecosystem using a third-party supplier, such as a third-party administrators or software providers, the third parties will apply the technical standards on behalf of their client pension providers and schemes or pensions dashboard providers. We expect much of the implementation of our standards will be undertaken by these third parties on behalf of multiple clients. A pension provider or scheme or a pensions dashboard provider connecting via an already-connected third party will use the third party's processes to meet the standards. However, as the standards apply to the pension provider or scheme or the dashboard provider, the latter are responsible for compliance with them, even if implementation is delegated to a third party. When we refer to pension providers and schemes and dashboard providers, this includes any of these third parties.

Jurisdiction

12. These standards apply to all United Kingdom pension providers subject to the dashboard duties in the FCA Rules, all United Kingdom schemes subject to the dashboard duties in the DWP Regulations, and all qualifying pensions dashboard service providers meeting the conditions in the DWP Regulations.

Use and evidence

13. Standards are mandatory requirements and, therefore, compliance by pension providers and schemes and by pensions dashboard service providers is compulsory.

14. Standards may be admitted in any proceedings relevant to pension providers and schemes and pensions dashboard providers' compliance with their duties. This applies to the obligations owed by any other party. For example, a pension provider's sponsoring employer or administrator. The body hearing the proceedings, including the FCA or The Pensions Regulator (TPR), will decide to assess the evidential weight attached to any standard or guidance admitted.

Version

15. This is version 1.1 of the draft code of connection. Refer to the [changelog](#) for updates since the last publication.

1. Security standards

PDP has developed a set of baseline security controls (BSC) for the ecosystem which are to be implemented for both the PDP (on behalf of MaPS) central digital architecture platform and for all connecting pension providers and schemes and Qualifying Pensions Dashboard Service (QPDS).

Note: In all cases where this document refers to pension schemes and providers as the entities on whom the obligation applies, while they are legally accountable for compliance, if the pension scheme or provider elects to connect via a contracted third party rather than connecting directly to the ecosystem, the third party will implement the requirement on the pension provider or scheme's behalf.

1.1 Technical security standards

CoCo1.1.1

- **Applies to:** Pension providers and schemes and QPDS.
- **Requirement:** Must implement at a minimum and must always support Transport Layer Security (TLS) encryption profile 1.2 for all ecosystem communication. Where a connection is successfully established between both parties using v1.3, they must not fall back to 1.2.
- **Reason for requirement:** Mandatory security control.

CoCo1.1.2

- **Applies to:** Pension providers and schemes and QPDS.
- **Requirement:** Must implement Mutual TLS (mTLS) encryption for all system-to-system communication within the ecosystem.
- **Reason for requirement:** Mandatory security control.

CoCo1.1.3

- **Applies to:** Pension providers and schemes and QPDS.
- **Requirement:** For any Public Key Infrastructure (PKI) you must be able to use the Elliptic Curve Digital Signature Algorithm (ECDSA) algorithms.
- **Reason for requirement:** Mandatory security control.

CoCo1.1.4

- **Applies to:** Pension providers and schemes and QPDS.
- **Requirement:** Should encrypt data at rest in accordance with industry good practice and are responsible for choosing the most appropriate encryption standard to protect sensitive data.

- **Reason for requirement:** Mandatory security control.
-

1.2 Security compliance standards

CoCo1.2.1

- **Applies to:** Pension providers and schemes and QPDS.
 - **Requirement:** Initial IT Health Check must be carried out by an independent third-party scheme accredited by either the Council of Registered Ethical Security Testers (CREST) or CHECK approved organisation prior to connecting to the ecosystem.
 - **Reason for requirement:** Mandatory security control. Maintains the security and integrity of the ecosystem.
-

CoCo1.2.2

- **Applies to:** Pension providers and schemes and QPDS.
 - **Requirement:** Scope of the IT Health Check must cover as a minimum scope the new infrastructure and services introduced to connect to the ecosystem. This must include both 'external' connection testing of systems to prevent unauthorised access, and 'internal' testing to assess for vulnerabilities and ensure internal networks and systems are securely configured and properly maintained.
 - **Reason for requirement:** Mandatory security control. Maintains the security and integrity of the ecosystem.
-

CoCo1.2.3

- **Applies to:** Pension providers and schemes and QPDS.
 - **Requirement:** Must carry out an initial IT Health Check prior to connection, and these initial results must be reported to, and presented to the PDP security authority (PDPSA) to receive approval.
 - **Reason for requirement:** Mandatory security control. Maintains the security and integrity of the ecosystem.
-

CoCo1.2.4

- **Applies to:** Pension providers and schemes and QPDS.
 - **Requirement:** Must use the Common Vulnerability Scoring System (CVSS) scores for classifying vulnerabilities identified in annual IT Health Checks. Medium, High or Critical, must have a remediation plan in place and approved by the PDPSA. Any allowed exceptions must be remediated within 12 months and resolved by the subsequent re-test (see 1.2.6).
 - **Reason for requirement:** Mandatory security control.
-

CoCo1.2.5

- **Applies to:** Pension providers and schemes and QPDS.
 - **Requirement:** Must keep IT Health Checks and subsequent remediation plans for a period of 6 years. PDP reserves the right to request to see IT Health Checks and remediation plans to address identified issues.
 - **Reason for requirement:** Mandatory security control.
-

CoCo1.2.6

- **Applies to:** Pension providers and schemes and QPDS.
 - **Requirement:** Must annually re-take a CREST or CHECK accredited IT Health Check within 12 months after the initial test or any significant change to the infrastructure and services in scope, and report on the outcome of the IT health check to the PDPSA.
 - **Reason for requirement:** Mandatory security control. Maintains the security and integrity of the ecosystem.
-

CoCo1.2.7

- **Applies to:** Pension providers and schemes and QPDS.
 - **Requirement:** Must carry out a retest of an IT Health Check on the request of the PDPSA.
 - **Reason for requirement:** Mandatory security control. Maintains the security and integrity of the ecosystem.
-

1.3 Security monitoring and incident response

CoCo1.3.1

- **Applies to:** Pension providers and schemes and QPDS.
 - **Requirement:** Must collect and retain event data and undertake activities that will help detect actual or potential security incidents and must have a protective monitoring policy that describes the use cases you are aiming to detect, which can be used to define event data collection. The policy must include both detection of technical attacks as well as important abuses of business processes.
 - **Reason for requirement:** Mandatory security control. Helps reduce the impact of security incident on the ecosystem.
-

CoCo1.3.2

- **Applies to:** Pension providers and schemes and QPDS.
 - **Requirement:** Must have a security incident management plan, which you should test periodically. This will include named responsible owners and pre-defined processes to respond to common forms of attack.
 - **Reason for requirement:** Mandatory security control. Helps reduce the impact of security incident on the ecosystem.
-

CoCo1.3.3

- **Applies to:** Pension providers and schemes and QPDS.
 - **Requirement:** For incidents that impact on PDP ecosystems or other participants, you must report them to the PDPSA team and other entities as required, within 24 hours of identification. Incidents should be reported to PDP security authority PDPSA@maps.org.uk.
 - **Reason for requirement:** Mandatory security control. Helps reduce the impact of security incident on the ecosystem.
-

CoCo1.3.4

- **Applies to:** Pension providers and schemes and QPDS.
 - **Requirement:** Should contribute threat intelligence relating to the ecosystem security to the PDPSA, and receive and act appropriately on intelligence received from the PDPSA. Incidents should be reported to PDP security authority PDPSA@maps.org.uk.
 - **Reason for requirement:** Mandatory security control. Helps reduce the impact of security incident on the ecosystem.
-

2. Service standards

CoCo2.1.1

- **Applies to:** Pension providers and schemes.
 - **Requirement:** Must acknowledge receipt of find requests by the find interface, by means of ACK (see technical standards) in <2 seconds (99.9% of ACK responses to acknowledge receipt of a find request to be returned in <2 seconds, measured over a 24 hour period). ACK response time is the time lapse between receiving the find request from the pension finder service and sending the ACK.
 - **Reason for requirement:** Effective traffic management. ACK is a synchronous automatic response to confirm receipt of the find request.
-

CoCo2.1.2

- **Applies to:** Pension providers and schemes.
- **Requirement:**
 - Must complete responses to find requests, including registering any pension identifiers (see [technical standards](#)).
 - For positive matches (including both matches made and possible matches; negative responses are not required) with the consent and authorisation service in <60 seconds following sending of the ACK.
- **Reason for requirement:**
 - User experience. Finding users' pensions is designed to be an in-session experience.
 - Efficient traffic management. Pension provider or scheme architectural optionality. 60 seconds does not require a particular architectural solution and supports searching across distributed systems as well as centralized architectural solutions.

- Pension provider or scheme burden. Registration of matches in response to find requests is a synchronous response, requiring pension providers and schemes to undertake matching and register a pension identifier for any found pensions.
-

CoCo2.1.3

- **Applies to:** Pension providers and schemes.
 - **Requirement:**
 - Must respond to view requests in <10 seconds (99.9% of view data payloads retrieved from systems and returned to the dashboard that issued the view request returned in <10 seconds, measured over a 24 hour period). View request response time is the time lapse between receipt of a dashboard view request and return of the view data payload (this includes the authorisation call to the consent and authorisation service to check authorisation of the view request).
 - View response time applies regardless of the view data payload. For example, whether the values are returned immediately in response to the view request, or whether a 3/10 working day calculation period applies. If the pension provider/scheme uses the permitted 3/10 working day period to calculate the values, the initial view response (comprising of the administrative data and signpost data, accompanied by the relevant ERI/accrued value unavailable code in the data standards) must still be <10 seconds.
 - Where a subsequent view request is received and a new calculation is required for a subsequent return of view data and the values cannot therefore be provided immediately (that is, the values have not been generated for a statement provided to the member within the past 13 months, or is based on a calculation made within the past 12 months), the values must be calculated and made available for return to dashboards within the same calculation timeframe as required by the Regulations ([Regulation 26\(5\)](#)) and FCA rules ([COBS 19.11.29](#)): 3 working days where all the benefits are money purchase benefits; 10 working days for all other cases. While the legislation sets the clock for the return of the first values to the registration of the pension identifier, for subsequent returns more than 3/10 working days after the registration of the pension identifier where values are not available for immediate return and new calculations are needed, the values must be made available for return within this timeframe from the point of receipt of the subsequent view request.
 - **Reason for requirement:**
 - User experience. Viewing pensions information is designed to be an in-session experience.
 - Architectural optionality. 10 seconds supports return of real-time data by means of APIs to retrieve data from pension provider or administration platforms.
 - Return of view data is a synchronous response.
-

CoCo2.1.4

- **Applies to:** Pension providers and schemes.
 - **Requirement:** Must restore service within 2 hours in the event of an endpoint outage, without loss of data ACKed before the outage.
 - **Reason for requirement:** User experience. Pensions dashboards are a digital service. Efficient traffic management.
-

CoCo2.1.5

- **Applies to:** Pension providers and schemes.

- **Requirement:**
 - Must be available 99.5%, 24/7, measured on a (calendar) monthly basis.
 - For clarity, 99.5% availability means 0.5% unavailability for whatever reason.
 - **Reason for requirement:** User experience. Pensions dashboards are a digital service. The central digital architecture will be available 99.5% 24/7.
-

CoCo2.1.6

- **Applies to:** Pension providers and schemes and QPDS.
 - **Requirement:**
 - Must generate, send, receive and retain unique transaction identifiers and timestamps in audit logs for all API interactions between ecosystem parties.
 - Transaction identifiers must be generated by the party initiating the transaction in accordance with the technical standards, issued to the other party to the transaction via the relevant API in accordance with the technical standards, and retained in the audit logs of both parties to the transaction for 6 years.
 - **Reason for requirement:** Ecosystem audit. Enables correlation of business audit logs across parties to support forensic investigation.
-

CoCo2.2.1

- **Applies to:** Pension providers and schemes.
 - **Requirement:** Must give a minimum of 5 working days' notice in advance of a scheduled service unavailability. Service unavailability includes any gap in service due to the service being unavailable or impaired.
 - **Reason for requirement:** Effective service management.
-

CoCo2.2.2

- **Applies to:** Pension providers and schemes.
 - **Requirement:**
 - Must notify PDP as soon as possible if a pension identifier for a match made must be de-registered (because the member has ceased to be a relevant member as defined in the legislation), but the protection API access token has expired, and the pension provider is therefore unable to de-register the pension identifier using the pension identifier registration API.
 - Must immediately stop serving view data for any view requests against pension identifiers that have been de-registered with the consent and authorisation service, or that have been flagged to PDP as requiring de-registration, but the provider is unable to de-register due to Protection API Token (PAT) expiry.
 - **Reason for requirement:** User experience. Mitigates the risk of find requests not being processed without the user's knowledge, resulting in pensions not being found.
-

3. Operational standards

CoCo3.1.1

- **Applies to:** Pension providers and schemes and QPDS.
 - **Requirement:** Must nominate and provide PDP with contact details for the following:
 - primary business contact
 - primary technical contact
 - security lead
 - test manager
 - service manager
 - **Reason for requirement:** Effective management of the ecosystem.
-

CoCo3.1.2

- **Applies to:** Pension providers and schemes.
 - **Requirement:** Must provide data required to register with PDP (MaPS) as a pension provider or scheme:
 - scheme name
 - regulator-issued registration code
 - regulator number
 - regulating body
 - holdername (see [technical standards](#))
 - holdername view endpoint (view_data_host_url)
 - details for the pension provider or scheme find-requests endpoint (find_request_path_url)
 - view-data endpoint
 - refresh endpoint
 - **Reason for requirement:** Ensuring connection of legitimate parties only.
-

CoCo3.1.3

- **Applies to:** QPDS.
 - **Requirement:** Must provide data required to register with PDP (MaPS) as a QPDS:
 - regulator-issued registration code
 - regulator number
 - dashboard redirect URL
 - dashboard user-managed access (UMA) claims redirect URL
 - **Reason for requirement:** Ensuring connection of legitimate parties only.
-

CoCo3.1.4

- **Applies to:** Pension providers.
- **Requirement:** Must supply PDP with their Firm Reference Number (FRN) and name as registered with the Financial Conduct Authority (FCA).
- **Reason for requirement:** Ensuring connection of legitimate parties only.

CoCo3.1.5

- **Applies to:** Pension schemes.
 - **Requirement:** Must supply PDP with their Pension Scheme Reference (PSR) number and name as registered with the Pensions Regulator (TPR).
 - **Reason for requirement:** Ensuring connection of legitimate parties only.
-

CoCo3.1.6

- **Applies to:** Pension providers and schemes.
 - **Requirement:** Must supply PDP with:
 - first name
 - last name
 - email address of the initial contact undertaking the preregistration process
 - the primary business contacts (if different to the initial contact)
 - the primary technical contact
 - **Reason for requirement:**
 - As part of the preregistration process PDP will validate the details provided directly with the pension scheme of provider, using a trusted contact provided to PDP from the relevant regulator.
 - Identity checks will be undertaken by PDP for the initial contact undertaking the preregistration process, the primary business contacts (if different to the initial contact) and the primary technical contacts, including when new primary business or primary technical contacts are added. The identity check will validate both the identity of the individual and their organisation email address.
 - Due diligence checks of the connecting organisation (ISP, pension provider or pension scheme) will be undertaken by PDP using data from company registers.
 - Providers and schemes must meet with the PDP engagement and technical teams as part of this process.
-

CoCo3.1.7

- **Applies to:** Pension providers and schemes.
 - **Requirement:** Must execute the test suite provided by PDP in participants own environment and submit successful test evidence through Salesforce in accordance with the PDP test pack.
 - **Reason for requirement:** Effective management of the ecosystem.
-

CoCo3.1.8

- **Applies to:** Pension providers and schemes.
 - **Requirement:** Must participate with PDP during the execution of the PDP test suite in the PDP pre-production environment. Submit test evidence through Salesforce in accordance with the PDP test pack.
 - **Reason for requirement:** Effective management of the ecosystem.
-

CoCo3.1.9

- **Applies to:** Pension providers and schemes.
 - **Requirement:** Must execute operational acceptance testing (OAT) test scripts, as documented in the PDP test pack to prove successful connection prior to live acceptance.
 - **Reason for requirement:** Effective management of the ecosystem.
-

CoCo3.1.10

- **Applies to:** Pension providers and schemes.
 - **Requirement:** Must provide a transition or implementation plan (steps).
 - **Reason for requirement:** PDP is required to ensure that the provider has identified the correct steps to enable them to connect. This is standard practice for IT changes. This would need to be reviewed by our technical team, who would need the ability to request further detailed if they are not satisfied that this connection would be safe for our ecosystem.
-

CoCo3.1.11

- **Applies to:** Pension providers and schemes.
 - **Requirement:** Must provide implementation team roles or responsibilities and contact details (if not part of the transition plan).
 - **Reason for requirement:** Ensuring connection of legitimate parties only.
-

CoCo3.1.12

- **Applies to:** Pension providers and schemes.
 - **Requirement:** Must provide a release note.
 - **Reason for requirement:** Ensuring connection of legitimate parties only.
-

CoCo3.1.13

- **Applies to:** Pension providers and schemes.
 - **Requirement:** Must provide proposed transition date.
 - **Reason for requirement:** Ensuring connection of legitimate parties only.
-

CoCo3.1.14

- **Applies to:** Pension providers and schemes.
 - **Requirement:** Must provide back out plan.
 - **Reason for requirement:** Ensuring connection of legitimate parties only.
-

CoCo3.1.15

- **Applies to:** Pension providers and schemes.
 - **Requirement:** Must evidence security authority criteria is satisfied.
 - **Reason for requirement:** Ensuring connection of legitimate parties only.
-

CoCo3.1.16

- **Applies to:** Pension providers and schemes.
 - **Requirement:** Must provide outstanding defects or issues.
 - **Reason for requirement:** Ensuring connection of legitimate parties only.
-

CoCo3.1.17

- **Applies to:** Pension providers and schemes.
 - **Requirement:** Must provide service transition plan.
 - **Reason for requirement:** Ensuring connection of legitimate parties only.
-

CoCo3.1.18

- **Applies to:** Pension providers and schemes.
 - **Requirement:** Must provide evidence that internal service acceptance has been carried out.
 - **Reason for requirement:** Ensuring connection of legitimate parties only.
-

CoCo3.2.1

- **Applies to:** Pension providers and schemes and QPDS.
 - **Requirement:** Must have a defined remediation route for service level failures.
 - **Reason for requirement:** Effective management of the ecosystem.
-

CoCo3.2.2

- **Applies to:** Pension providers and schemes and QPDS.
 - **Requirement:** Must have internal escalation frameworks and processes. Ensure staff know how, and who, internal issues should be escalated to and when.
 - **Reason for requirement:** Effective management of the ecosystem.
-

CoCo3.2.3

- **Applies to:** Pension providers and schemes and QPDS.

- **Requirement:** Must have a framework for raising issues and monitoring issues to resolution.
 - **Reason for requirement:** Effective management of the ecosystem.
-

CoCo3.2.4

- **Applies to:** Pension providers and schemes and QPDS.
 - **Requirement:** Must make all reasonable efforts to support forensic investigation where required, including supporting mediated access to business audit logs.
 - **Reason for requirement:** Effective management of the ecosystem.
-

CoCo3.2.5

- **Applies to:** Pension providers and schemes.
 - **Requirement:** Must ensure that any contracted third parties managing connection to the ecosystem on behalf of the pension provider or scheme severs the connection of the pension provider or scheme if directed by PDP. For example, where the pension provider or scheme ceases to have any relevant members, or if the provider ceases to be registrable with the regulator.
 - **Reason for requirement:** Ensuring only relevant pension providers and schemes remain connected to the of the ecosystem.
-

CoCo3.2.6

- **Applies to:** Pension providers and schemes and QPDS.
 - **Requirement:** Must keep key contacts (see CoCo3.1.1) up to date at all times via the PDP connection portal on Salesforce and communicate any personnel changes to PDP immediately.
 - **Reason for requirement:** Effective management of the ecosystem.
-

CoCo3.2.7

- **Applies to:** Pension providers and schemes.
- **Requirement:** Must keep pension provider registration data (see CoCo3.1.2) up to date at all times and inform PDP immediately of any changes. For example, as a result of mergers and acquisitions.
- **Reason for requirement:** Effective management of the ecosystem.