

Code of connection

The code of connection sets out how pension providers and schemes connect to the dashboards ecosystem and what they need to do to remain connected. It provides assurance that the systems and services of all participants in the ecosystem are managed and controlled to the appropriate levels. It comprises connection standards, security standards, technical standards, service standards and operational standards.

Version 2.0

These standards are approved by the Secretary of State for Work and Pensions and the Department for Communities (Northern Ireland) and were published on **13 March 2025**.

Pension providers and schemes must align with this version of the code of connection.

These standards were approved by the Secretary of State for Work and Pensions on 4 March 2025 and by the Department for Communities (Northern Ireland) on 13 March 2025.

How changes to standards will be managed will be outlined in PDP's [approach to standards governance](#).

Changelog

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, occupational and personal pensions. This supports individuals' engagement with their pensions and their retirement planning.
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 is 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 (No 2) Regulations (Northern Ireland) 2023 (referred to hereafter as 'Regulations') and the Rules of the Financial Conduct Authority (FCA) (hereafter 'Rules').

6. The code of connection sets out requirements that must be met to connect to the pensions dashboards ecosystem and to remain connected. It consists of standards that are distinct, for legislative purposes, but are gathered together in one code of connection setting out all the connection and service requirements in one place. The code of connection comprises:

- connection standards
- security standards
- technical standards
- service standards
- operational standards

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.

Application

9. These standards apply legally to the trustees or scheme managers of occupational pension schemes (pension schemes) and the managers of stakeholder and personal pension schemes (pension providers) connected to, or required to connect to, the pensions dashboards ecosystem. This version does not include any standards that apply to dashboard providers. The standards for dashboard providers will be published separately.

10. The code of connection standards are important for pension providers and schemes to understand, whether they are connecting directly to the ecosystem or connecting using a third-party supplier such as third-party administrators or software providers (integrated service providers, or ISPs). In these cases, third parties will apply the standards, by sending the data to MaPS, on behalf of their client pension providers and schemes. PDP expects much of the implementation of the standards will be undertaken by these third parties on behalf of multiple clients. A pension provider or scheme connecting via an already-connected third party will use the third party's processes to meet our standards. However, as the standards apply to the pension provider or scheme, the pension provider or scheme is responsible for compliance with them, even if implementation is delegated to a third

party. When referring to pension providers and schemes, this includes any of these third parties.

Jurisdiction

11. These standards apply to all United Kingdom pension providers subject to the dashboard duties in the FCA Rules for pension providers, and all United Kingdom pension schemes subject to the dashboard duties in the Regulations.

Other standards

12. These standards should be read in conjunction with the other [PDP standards](#) (technical standards, data standards and reporting standards).

Compliance

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

Version

14. This is the version 2.0 of the code of connection. Refer to the [changelog](#) for updates since the last publication.

1. Security of the dashboards ecosystem

1.1 Securing ecosystem communication (technical standards)

CoCo1.1.1

- **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:** Security control to maintain the security and integrity of the ecosystem.
-

CoCo1.1.2

- **Requirement:** Must implement Mutual TLS (mTLS) encryption for all system-to-system communication within the ecosystem.
 - **Reason for requirement:** Security control to maintain the security and integrity of the ecosystem.
-

CoCo1.1.3

- **Requirement:** Must use the Elliptic Curve Digital Signature Algorithm (ECDSA) algorithms for any Public Key Infrastructure (PKI).
 - **Reason for requirement:** Security control to maintain the security and integrity of the ecosystem.
-

CoCo1.1.4

- **Requirement:** Should encrypt data at rest in accordance with industry good practice. Parties are responsible for choosing the most appropriate encryption standard to protect sensitive data.
 - **Reason for requirement:** Security control to maintain the security and integrity of the ecosystem.
-

1.2 Security testing (security standards)

CoCo1.2.1

- **Requirement:** Must undergo an initial IT Health Check, performed 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:** Security control to maintain the security and integrity of the ecosystem.
-

CoCo1.2.2

- **Requirement:** Must ensure the scope of the IT Health Check covers 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:** Security control to maintain the security and integrity of the ecosystem.
-

CoCo1.2.3

- **Requirement:** Must report IT Health Check results to MaPS, and present on the findings to MaPS to receive approval.
 - **Reason for requirement:** Security control to maintain the security and integrity of the ecosystem.
-

CoCo1.2.4

- **Requirement:** Must use the Common Vulnerability Scoring System (CVSS v3 or higher) 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:** Security control to maintain the security and integrity of the ecosystem.
-

CoCo1.2.5

- **Requirement:** Must keep IT Health Checks and subsequent remediation plans for a period of 6 years. MaPS reserves the right to request to see IT Health Checks and remediation plans to address identified issues.
 - **Reason for requirement:** Security control to maintain the security and integrity of the ecosystem.
-

CoCo1.2.6

- **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 to MaPS.
 - **Reason for requirement:** Security control to maintain the security and integrity of the ecosystem.
-

CoCo1.2.7

- **Requirement:** Must carry out a retest of the IT Health Check on the request of MaPS.
 - **Reason for requirement:** Security control to maintain the security and integrity of the ecosystem.
-

1.3 Security monitoring and incident response (security standards)

CoCo1.3.1

- **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. This policy must include both detection of technical attacks as well as important abuses of business processes.
 - **Reason for requirement:** Security control to help reduce the impact of security incident on the ecosystem.
-

CoCo1.3.2

- **Requirement:** Must have a security incident management plan, which you should test periodically. This must 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.
-

1.3 Security monitoring and incident response (service standards)

CoCo1.3.3

- **Requirement:** Must report incidents that impact on the dashboards ecosystem or other participants to MaPS and other entities as required, within 24 hours of identification. Intelligence and incidents should be reported to MaPS at PDPSA@maps.org.uk.
 - **Reason for requirement:** Security control to help reduce the impact of security incident on the ecosystem.
-

CoCo1.3.4

- **Requirement:** Must contribute threat intelligence relating to the ecosystem security to MaPS, and receive and act appropriately on intelligence received from MaPS. Incidents should be reported to MaPS at PDPSA@maps.org.uk.
 - **Reason for requirement:** Security control to help reduce the impact of security incident on the ecosystem.
-

2. Service levels and required behaviour

2.1 Service response times, availability requirements and service restoration requirements (technical standards)

CoCo2.1.1

- **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

- **Requirement:** Must complete responses to find requests, including registering any pension identifiers (see [technical standards](#)) within 60 seconds for positive matches (including both matches made and possible matches; negative responses are not required) 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

- **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 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 or scheme uses the permitted 3/10 working day period to calculate the values, the initial view response (comprising the administrative data and signpost data, accompanied by the relevant ERI/accrued value unavailable code in the data standards) must still be <10 seconds.
 - **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.
-

2.1 Service response times, availability requirements and service restoration requirements (connection standards)

CoCo2.1.4

- **Requirement:** Must target restoring 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

- **Requirement:**
 - Must target availability of at least 99.5%, 24/7, measured by calendar month.
 - 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

- **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.

CoCo2.1.7

- **Requirement:** Must, where a view request is received and a new calculation is required for return of the value data and the values cannot therefore be provided immediately (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), calculate the values and make them 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](#)). For example, 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 3/10 working days, from the day after the receipt of the view request.
- **Reason for requirement:** Align timing for subsequent calculations with the calculation times for initial calculations set out in legislation.

2.2 Service notifications (service standards)

CoCo2.2.1

- **Requirement:** Must give a minimum of 5 working days' notice to MaPS 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

- **Requirement:** Must notify MaPS (through the connecting organisation, not directly from pension provider or scheme to MaPS, if connecting via a third party) as soon as possible of any change in connection arrangements. This includes changes 'internal' to the connection solution used, such as moving from a data lake ISP model for processing of find or view requests to using a federated model with onward connectivity between ISP and provider or scheme.
- **Reason for requirement:** Effective management of the ecosystem.

3. Procedural requirements for connection

3.1 Onboarding (operational standards)

CoCo3.1.1

- **Requirement:** Must nominate and provide MaPS 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

- **Requirement:** Must provide data required to register with MaPS as a pension provider or scheme:
 - pension provider or 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.
-

CoCo3.1.4

- **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

- **Requirement:** Must supply MaPS 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 MaPS will validate the details provided directly with the pension scheme or provider, using a trusted contact provided to MaPS from the relevant regulator.
 - Identity checks will be undertaken by MaPS 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.

3.1 Onboarding (connection standards)

CoCo3.1.7

- **Requirement:** Must execute the test suite provided by MaPS in participants' own environment and submit successful test evidence through the MaPS connection portal of Salesforce in accordance with the MaPS test pack.
- **Reason for requirement:** Effective management of the ecosystem.

CoCo3.1.8

- **Requirement:** Must participate with MaPS during the execution of the test suite in the MaPS pre-production environment. Submit test evidence through the MaPS connection portal of Salesforce in accordance with the MaPS test pack.
- **Reason for requirement:** Effective management of the ecosystem.

CoCo3.1.9

- **Requirement:** Must participate with MaPS to execute operational acceptance testing (OAT) in the production environment, to prove successful connection prior to live acceptance.
- **Reason for requirement:** Effective management of the ecosystem.

3.1 Onboarding (operational standards)

CoCo3.1.10

- **Requirement:** Must provide a transition or implementation plan (steps).
- **Reason for requirement:** MaPS 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 the technical team, who would need the ability to request further details if they are not satisfied that this connection would be safe for our ecosystem.

CoCo3.1.11

- **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

- **Requirement:** Must provide a release note.
 - **Reason for requirement:** Ensuring connection of legitimate parties only.
-

CoCo3.1.13

- **Requirement:** Must provide proposed transition date.
 - **Reason for requirement:** Ensuring connection of legitimate parties only.
-

CoCo3.1.14

- **Requirement:** Must provide a backout plan.
 - **Reason for requirement:** Ensuring connection of legitimate parties only.
-

CoCo3.1.15

- **Requirement:** Must provide outstanding defects or issues.
 - **Reason for requirement:** Ensuring connection of legitimate parties only.
-

CoCo3.1.16

- **Requirement:** Must provide service transition plan.
 - **Reason for requirement:** Ensuring connection of legitimate parties only.
-

CoCo3.1.17

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

3.2 Business as usual service maintenance requirements (operational standards)

CoCo3.2.1

- **Requirement:** Must have and upon request provide MaPS with a defined remediation route for service level failures.
 - **Reason for requirement:** Effective management of the ecosystem.
-

CoCo3.2.2

- **Requirement:** Must have and upon request provide MaPS with internal escalation frameworks and processes. Ensure staff know how, to whom and when internal issues should be escalated.
 - **Reason for requirement:** Effective management of the ecosystem.
-

CoCo3.2.3

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

CoCo3.2.4

- **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.
-

3.2 Business as usual service maintenance requirements (connection standards)

CoCo3.2.5

- **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 MaPS. 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 ecosystem.
-

3.2 Business as usual service maintenance requirements (service standards)

CoCo3.2.6

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

CoCo3.2.7

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