Pensions Dashboards Programme

Dashboard selection criteria questionnaire

Background

We would like to know more about your company and to understand your motivation for presenting a pensions dashboard. This information will help us ensure that we are selecting an appropriate range of presentation options during the alpha phase of the project. Similarly, we are keen to ensure that organisations are able to deliver a dashboard in the relatively short timeframe required to support alpha testing.

If you are not selected for the alpha phase, you can still participate in the future and we will be actively looking to recruit participants for our subsequent beta phase in due course.

Your Organisation:

Company name
Contact name
Contact email address
Contact phone number

Companies House registration
ICO Data Protection registration
FCA Registration

Q1. Tell us about your organisation and your aims for your dashboard
- **1.1** What is the size of your organisation, by employees and turnover?
- **1.2** What are your key organisational objectives?
- **1.3** What products and services do you currently plan to provide?
- **1.4** How will your dashboard support your existing services?

Q2. Tell us about your client base, both current and future planned
- **2.1** What is your existing client base, by volume and demographic?
- **2.2** How do you think your dashboard will:
  - **a)** enhance your customer experience
  - **b)** influence your target demographic

Understanding of the pensions market

Diversity and innovation are key to providing consumers with choice in how they receive their pension information. PDP recognises and welcomes the fact that not all dashboard providers will have a history in the pensions industry or a deep understanding of the way in which pensions have evolved.

This section will not form a part of the formal assessment of suitability but will help the programme understand the breadth of applicants.

Q3. Please describe the extent of your previous engagement with the pensions industry.

Q4. Do you have access to resource that will support your understanding of the pensions market during the development of your pensions dashboard?

Consumer engagement

The Pensions Dashboards Programme (PDP) would like to understand the ways in which your organisation ensures that the services you provide are appropriate for the needs of target users.

Q5. With reference to your services mentioned in Question 1.3, could you confirm whether:
- **5.1** they are user facing
- **5.2** they include any financial services products

Q6. Please describe your approach to gathering user needs and/or viewpoints
- **6.1** How do you use this insight to influence the design of your services/propositions?
- **6.2** How do you ensure that your products and services remain relevant and appropriate to consumers?

Q7. Please provide an overview of your product development process (this relates to product/service evolution and not feature development).

Q8. Please advise whether you are willing to share any existing user research that you may have undertaken with:
- **8.1** the Pensions Dashboards Programme
- **8.2** working groups, including other dashboard providers

Collaborative working with PDP

The Pensions Dashboards Programme will continue to evolve technical and design standards during the alpha phase of the programme. It is important that our partners contribute to this process and bring the benefit of their experience into this collaborative approach.

Q9. Please provide details of the resources that you have to support your participation in the alpha phase.

9.1 Will your resources be made available for workshops, working groups and collaborative sessions?

9.2 Please describe your approach to finding and deploying test resource – both internal and external.

Q10. Please provide an overview of any collaborative initiatives in which you have participated (we recognise that there may be intellectual property limitations to what you can disclose).

Q11. What are your views on sharing your research and findings:

11.1 on the development of your pensions dashboard?

11.2 from earlier development of your services?

Q12. Within a collaborative environment you will be asked to:

a) operate fairly and without prejudice with all participating parties, including PDP, other technology suppliers and other dashboard providers

b) sign and maintain confidentiality agreements

c) commit to and support joint communication plans

d) participate in a joint testing community

12.1 Please confirm whether you will be able to support all of these requirements

Capability

Your technical and delivery capability will be key to supporting the test phases of the ecosystem development. PDP is keen to work with responsive partners, which have demonstrable processes that enable effective management of issues and development.

To be selected for alpha, you will be required (at a minimum) to meet our Security and technology checklist (appendix)

Q13. Does your organisation comply with all aspects of the checklist:

13.1 Yes / No?

13.2 If no, which elements do you not currently meet?

13.3 Please describe whether you plan to make meet these criteria and, if yes, what the target date is for completion.

Q14. Please describe the tech stack you propose to operate dashboards on.

Q15. Please describe your organisation's approach to software development, including descriptions of your software development methods, organisation, tooling and lifecycle.

Q16. Tell us about your approach to conforming with security models and standards.

16.1 Are you certified, if yes, to which standard?

16.2 Please demonstrate your approach to security by design.

16.3 Do you operate defined security roles and responsibilities within the organisation and are they aligned with the delivery of a dashboard?

Q17. Please provide an overview of your test approach, including:
- **17.1** structure and roles
- **17.2** phases and methods
- **17.3** dedicated test tools utilised
- **17.4** specialist security testing capability

Q18. Please describe your organisation's approach to penetration (pen) testing.
- **18.1** What is the scope of your pen testing?
- **18.2** Please advise which organisation undertakes your pen tests?
- **18.3** Please provide a summary of your last relevant pen test – including the status of any high or critical findings.

Q19. Do you internally test for OWASP Top ten?

Q20. Please outline your defect management approach:
- **20.1** Do you utilise any defect management tools?
- **20.2** How do you manage and track requirements?

Q21. Please describe your approach to non-functional testing.
- **21.1** Which tools do you utilise to complete non-functional testing?

Q22. Please outline your backup and DR solution.

Q23. Please outline your operations capacity model, including how it is updated and validated.

Q24. Could you please describe your current service model:
- **24.1** Does your model include a help desk? If so, please describe its structure and how it can be enhanced to support the pensions dashboard.
- **24.2** Is your service ISO20001 accredited?
- **24.3** What changes will your service model need to support your pensions dashboard?

Q25. Please provide a data model/dictionary for your service.

Q26. Please tell us about any software development initiatives and experience your organisation has within financial services. A statement of experience would be useful.
- **26.1** Provide three recent (ie within the last three years) client site references, with assurances that there are no potential conflict of interests with any client references.

Q27. Please outline your organisation's potential policies and ability to preserve data sovereignty.

Governance and legal

In the future, the provision of pensions dashboards will be regulated by the Financial Conduct Authority (FCA). This regulatory responsibility will not be in place until the relevant legislation has passed through government. In the interim, PDP may require your organisation to make certain commitments:

Q28. Would your organisation willingly sign consumer protection measures ahead of regulation?

Q29. Has your organisation completed any data protection impact assessment (DPIA) or do you have plans to do so?

29.1 Can your DPIA be shared with PDP?

Q30. Would your organisation be willing to work alongside PDP, DWP and the FCA to:

30.1 support the development of the rules and regulations applied to dashboard provision?

30.2 test governance and registration approaches?

30.3 evidence the ways in which personal data will be used by dashboard providers?

30.4 develop the programme's liability model and the way in which it can be applied practically?

Q31. Has your company been the subject of any complaint, legal proceedings, sanction or investigation by The Pensions Regulator, the Financial Conduct Authority or any other UK regulatory body?

31.1 Please declare any and all actions, even if the action was resolved in your favour.

31.2 Have you been subject to any regulatory action by any non-UK regulators?

Q32. Have you been the subject of any ICO complaint, sanction or legal proceedings irrespective of outcome? Please provide details.

Security and Technical Checklist

Security standards you must meet

#	Area	What?
1	NCSC CHECK IT Health Check or suitable equivalent	All controls shall be independently assured
2	X.509 certificates	Communication channels shall be checked for certificate issuance authenticity/validity
3	DNSSEC	Inter-domain communication shall have origin authentication and integrity checking for DNS.
4	OCSP	Inter-domain certificate-based identification should implement Online Certificate Status Protocol
5	TLS v1.3	TLS should be adopted on all communications
6	mTLS	Mutual Transport Layer Security (mTLS) implemented on all TLS channels
7	Datagram Transport Layer Security (DTLS) v 1.2	Asynchronous communications carrying attributable personal data shall be channel protected
8	AES-256 minimum FIPS 140-2.	Persistent storage shall be encrypted using AES-256 as a minimum Encryption keys should be stored within a Hardware Security Module (HSM) validated to FIPS 140-2 minimum.
10	DEK	Data Encryption Keys (DEK) shall be encrypted at rest. Data write operations shall be encrypted with a new DEK.

Technical areas you will need to work with

#	Area	What?
1	API gateway standards	Compliance with the e-2-e messaging standards is mandatory
2	UMA 2	Operate UMA Grant protocol for redirection to the claims endpoint and to obtain authorisation to retrieve pension details
3	Response times	We will be issuing some minimum SLAs for response to messaging to ensure the service is useable
4	Availability	We have high expectations of providing a high availability solution – 99.95%
5	Resilience	We expect all suppliers to provide resilient services
6	User design and Agile principles	PDP is an Agile project and has an expectation that suppliers will have user-focused development
7	Auto provisioning	We will have auto-provisioning services to give high certainty of controlling configuration and restoring the service quickly
8	Auto scaling	The platform will be auto scaling to manage any unexpected peaks in the public service
9	Incident management and helpdesks	We will have linked helpdesks, with well-defined triage and hand off processes to deal with incidents effectively
10	De-referencing PeI	Use configuration logic to resolve PeI into a URL in order to make the view request
11	Redirect user to C&A for user to re-consent	Dashboard will have logic to redirect the user to the C&A if their consent relating to management of their pension resource(s) by a data provider has expired