Key Outcomes

Title:	Digital Service Provider, Operational Framework Review Requirements & Lifecycle Management Focus Group		
Issue date:	6 May 2021		
Venue:	WEBEX		
Event date:	24 February 2021	**Start:** 11:00	**Finish:** 13:00

Chair:	Diana Porter	**Facilitator:**	Diana Porter
Contact:	Julie Huynh	**Contact phone:**	(02) 8894 9304

Intent:	Explore opportunities to improve process, guidance and documentation

Attendees:	ATO Kylie Johnston, Director Digital Partnership Office (DPO) Diana Porter, Operational Framework Lead, DPO Miranda Shaw, Director Information Cyber Security Operational Framework Team Industry Arrow Research Corporation Shaun Wilkinson ANZ Onepath David Delaney Class Super Philip Boadi ELMO Software Artur Czernecki Paypac Payroll Belinda Stewart Pronto Software Gary Semple Superchoice James Cameron Xero Matthew Prouse Xero Erin Adams Xero Helen MacGillivray
Apologies:	Toby Amodio, Director, Information & Cyber Security Claire Miller, Director, Digital Communication & Identity Services Paul Dwyer, Project Manager, Digital Wholesale Integration

	Industry	
	ANZ Onepath	David Delaney
	AMP	Andrew Strong
	BT Financial	Kim Sung Do
	Tanda	Roderick Schneider

Next meeting: TBA

The key outcomes for this meeting are best read in conjunction with the Requirements & Lifecycle Management focus group presentation and attachments.

Agenda item: Introduction

Two key themes were discussed including an overview of feedback from the first session on:

1. Supporting Guidance for Certification
    a. DSPs with multiple products including certification
    b. Enhancing certification for DSPs
    c. Guidance on indirect consumers and third-party applications
    d. Guidance on volume of records
2. Guidance and process on DSP Lifecycle Management
    a. Terms and Conditions relating to data breaches
    b. Improvements to Letter of Confirmation
    c. Improvements to Annual Review guidance and process
    d. Notification of Significant changes

Agenda item: 1 – Supporting guidance for certification

The group discussed previous feedback on supporting guidance for:

1. Supporting guidance for certification
    - ISO27002 was agreed by the group to be adopted as it may assist smaller DSPs in undertaking security certification.
    - Certification for DSPs with multiple products
    - DPO recognises there are occasions when multiple products will share infrastructure and certificates across their organisation. DPO will consider one response for multiple products when all the following factors are consistent across products:
        - Controlled by client or DSP
        - Services consumed
        - Risk rating of services
        - Volume of records greater or less than 10,000
        - This may include provision of supplementary evidence for any known gaps.
    - Suggestion to remove “greater or less than” in the volume of records factor.
    - An attestation to independent certification stating it includes the product under DSP Operational Framework (OPF) will be accepted as evidence of meeting the certification requirement.

- Enhancing certification for DSPs

- ISO27002 was discussed to be suitable self-certification standard to support smaller DSPs.
- Alternative standards including the Security Standard for Add-on Marketplaces (SSAM) and ISO27017 was discussed with the group with updates to the guidance material to be made.

- Guidance on indirect consumers and third-party applications
  - DPO is reviewing the scoping statement for the DSP Operational Framework to provide further guidance and include the word 'store'.
  - DSPs are only required to assess their own service as part of the DSP OPF requirements.

- Guidance on volume of records
  - Definition of "highly leveraged" to be amended to include "store or transmit" and to change "client" to "taxpayer".
  - A discussion on the origin of "highly leveraged" threshold (10,000 records). This threshold aligns with the need for independent certification.

Outcomes from industry discussion:

- A streamlined approach was supported by DSPs to reduce administrative burden.
- DPO agreed to provide additional guidance on ISO27002 self-assessment process within knowledge base of Online Services for DSPs (OLS4DSPs).
- When multiple products have the following factors one submission will be accepted.
- An attestation to independent certification stating it includes the product under DSP Operational Framework (OPF) will be accepted as evidence of meeting the certification requirement.

Further consideration is needed for:

- DPO will prepare guidance within knowledge base of OLS4DSPs relating to indirect consumers and third-party applications i.e. visual diagrams and ISO27002.

Agenda item: 2 – Guidance on DSP lifecycle management

The group discussed previous feedback on supporting guidance for:

2. Guidance on DSP lifecycle management
   - Terms & Conditions relating to data breaches
     - DSPs to contact DPO regarding a data breach through OLS4DSPs.
     - Early communication of potential breach is best practice. Not all information needs to be confirmed before communicating with DPO and impacted client, preference to notify DPO early so we can work with you.

   - Improvements to Letter of Confirmation
     - Updates to existing letter of confirmation made, DPO will acknowledge DSP Operational Framework requirements are met by including the DSP and product details.

   - Improvements to Annual Review process
     - No comments were made.

- Notification of significant changes
  - Notification of significant change will align to DSPs internal privacy policies.
  - DPO to provide further guidance within documentation on disclosures of mergers and acquisitions i.e. notify ATO on the day or as soon as commercially viable.

Outcomes from industry discussion:

- Updates to letter of confirmation, DPO will acknowledge DSP Operational Framework requirements are met by including the DSP and product details.
- No changes to Annual Review process.
- Updates to guidance material to reflect outcomes.

Further consideration is needed for:

- Scenarios to be created for DSPs within knowledge base of OLS4DSPs.

Agenda item: – Wrap Up & Next Steps

Outcomes of working group to be published and circulated.