# Key Outcomes



| | | | |
|---|---|---|---|
| **Title:** | Operational Framework Review<br>Focus Group – Requirements & Lifecycle Management | | |
| **Issue date:** | 3 December 2020 | | |
| **Venue:** | WEBEX | | |
| **Event date:** | 19 November 2020 | **Start:** 11:00 | **Finish:** 13:00 |

| | | | |
|---|---|---|---|
| **Chair:** | Diana Porter | **Facilitator:** | Diana Porter |
| **Contact** | Diana Porter | **Contact phone:** | (02) 4724 0528 |

| | |
|---|---|
| **Attendees: names/section** | ATO<br>Kylie Johnston - Director Digital Partnership Office<br>Diana Porter - Digital Partnership Office<br>Jarrod Wellings - Digital Partnership Office<br>Sangitha Sivayogaraj - Director, Digital Wholesale Integration<br>Benjamin Avery - DCIS Project Management<br>Ian Lloyd - Digital Partnership Office<br>Industry<br>Andrea Cooper - IRESS<br>Artur Czernecki – ELMO Software<br>Belinda Stewart – Paypac Payroll<br>Estevan Chaves – Sage Software Australia<br>Gary Semple – Pronto Software<br>Helen MacGillivray - Xero<br>James Cameron - SuperChoice<br>Karl Farrand - TaxLab<br>Matthew O'Loughlin – Ozedi Holdings<br>Matthew Prouse - Xero<br>Philip Boadi – Class Super<br>Sandeep Gopalan - GovReports<br>Shaun Wilkinson – Arrow Research Corporation |
| **Apologies: name/section** | Toby Amodio - Director, Information & Cyber Security<br>Claire Miller - Director, Digital Communication & Identity Services |

| | |
|---|---|
| | Paul Dwyer - Project Manager, Digital Wholesale Integration<br>Andrew Strong - AMP<br>David Delaney - ANZ Onepath<br>Kim Sung Do - BT Financial<br>Roderick Schneider - Tanda |

| | |
|---|---|
| **Next meeting** | TBA |

The key outcomes for this meeting are best read along with the Requirements & Lifecycle Management focus group presentation.

## Agenda item: 1 – Introduction

An overview of findings from independent review and DSP feedback included 3 opportunities to improve our requirements documentation & lifecycle management guidance.

These include:

1. supporting guidance for certification
2. improve guidance on encryption
3. guidance and process on DSP lifecycle management

It was recognised that some items in this working group will cover additional guidance and support documentation needed for particular items covered in other working groups where technical soultuons are also being considered. DPO will consider feedback from both groups when finalising updated guidance.

## Agenda item: 2 – Certification

Discussion on opportunities to improve guidance and support for DSPs to meet certification.

Key points from industry discussion and feedback included:

- Operational Framework is designed to be applied at the product level, however it is recognised when DSPs undertake certification it is sometimes applied across the whole organisation and can also include multiple products.
- Language for the certification requirements needs to improve:
    - Scope of certification - when it should be applied to the business and/or the product i.e. the application of certification for platforms with multiple products.
    - Definition of “tax and super data” that counts toward the volume threshhold for independent certification. Suggestion for business/ accounting/payroll etc vs tax/super data?

- Definition of indirect consumers of ATO APIs to determine if they are within scope.

Guidance should be provided around specific controls of standards like the ISO27001 which may benefit smaller DSPs.

## Agenda item: 3 – Encryption Guidance

Discussion on opportunities to improve documentation and to address any potential gaps.

- Encryption In Transit:
  - In alignment to the Australian Cyber Security Centre - Information Security Manual, support for TLS1.0 and TLS1.1 will be deprecated.
  - While many businesses in industry have already began to deprecate TLS1.0 and TLS1.1, it is challenging to ask on premise clients to uplift security of older operating systems which DSPs have no control over.
  - TLS1.2 and TLS1.3 is currently supported. DSPs can plan to transition to TLS1.3, but must use TLS1.2 as a minimum.
  - Streamlined evidence requirements by DSPs providing an SSL reports e.g. SSL labs only require TLS1.2 for an 'A' rating.
- Encryption at Rest:
  - Is further data encryption required when the S3 bucket is already encrypted as this is a significant cost to DSPs.
  - As technology improves and encryption at rest is applied by default, a re-evaluation is required to ensure intended risk mitigation.
- Encryption Key Management:
  - Agreement across the group on the proposed DPO improvements to guidance relating to encryption key management.

## Agenda item: 4 – Lifecycle Management

Discussion on improving guidance and process across various areas of the DSP lifecycle management fincluding terms & conditions, letter of confirmation, annual review process and the notification of change environment. Overall the group agreed the areas of concern could be improved. DPO will provide draft guidance for the group to review in the final working group meeting.

Key points and considerations from industry discussion and feedback included:

- Terms & Conditions:
  - 'Immediately' is currently being addressed.
  - Request to include 'marketplace or ecosystems' in T&C's as information is requested in the questionnaire.
- Letter of Confirmation:
  - Place a QR code on the letter to link to the standards/requirements the DSP has met.
- Annual review Process

    - Consider a DSP nominated period for annual review, to support each DSPs business requirements.
    - A ‘no changes’ check on the questionairre will save administrative copy & paste.
    - Improved/additional guidance for changing certification requirements i.e. moving from self-certification to independent certification and vice versa.
- Notification of Changes
    - Improve guidance/requirements for notification when there is a merger or acquisition.
    - DSPs to be notified when changes are made to published documentation (e.g. questionnaire, requirements) in addition to the DSP newsletter (due to the audience of the DSP newsletter).

**Agenda item: – Wrap Up & Next Steps**

Outcomes of the focus group to be published and circulated, members are encouraged to provide further feedback and comment.

ATO will establish a second meeting in December.