Australian Government
Australian Taxation Office

Digital Service Provider (DSP) Operational Framework Review

Requirements & Lifecycle Management Focus Group – Session 2

Presented by Diana Porter

24th February 2021

Recap on the groups aim and what we are trying to achieve

Explore opportunities to improve process, guidance and documentation relating to requirements and lifecycle management of the DSP Operational Framework

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 & Conditions relating to data breaches
b. Improvements to Letter of Confirmation
c. Improvements to Annual Review guidance and process
d. Notification of significant changes

1 Supporting Guidance for Certification

a. DSPs with multiple products including certification
b. Enhancing certification for DSPs
c. Guidance on In-direct consumers and Third Party Applications
d. Guidance on volume of records

1a DSPs with multiple products including certification

Streamlining Operational Framework for DSPs with multiple products.

CURRENT ENVIRONMENT

DSP Operational Framework Requirements to utilise ATO digital services (pg.5)

The DSP Operational Framework applies to each product/service. DPO recognises there are occasions when multiple products will share infrastructure and potentially certifications across their organisation.

WHATS NEW

Additional information to assist DSPs with multiple products

DPO will consider one response for multiple products when all of the following factors are consistent across products:

- Controlled by client or DSP
- Services consumed
- Risk rating of services
- Volume of records < or > 10,000

This may include provision of supplementary evidence for any known gaps.

1a DSPs with multiple products including certification

Providing additional guidance on certification for DSPs with multiple products.

CURRENT ENVIRONMENT

DSP Operational Framework Requirements to utilise ATO digital services (pg.16)

The scope of certification should cover relevant organisational policies, procedures and data repositories that hold or manage tax or superannuation related information.

WHATS NEW

Additional scoping guidance for DSPs with multiple products who require independent certification

The scope of certification should cover relevant organisational policies, procedures and data repositories that hold or manage tax or superannuation related information.

DPO will accept this as evidence across multiple products when the DSP can assert that each product is covered under the certification.

1b Enhancing certification for DSPs

Guidance should be provided around specific controls of standards which may benefit smaller DSPs in demonstrating alignment of their security posture.

CURRENT ENVIRONMENT

DSP Operational Framework Requirements to utilise ATO digital services (pg. 7 & 15-17)

DSPs are able to self-certify against one of the below:

- ISO 27001
- Australian Cyber Security Centre (ACSC) Information Security Manual (ISM), assessment against this standard is termed ‘iRAP’
- SOC 2
- OWASP ASVS 3.0 or later

WHATS NEW

DPO will now accept self certification of ISO 27002 as an additional standard for small DSPs operating with client controlled solutions. The requirements table and documentation will be updated to reflect this outcome.

DSPs to contact DPO to request to use an alternative security certification. Requests will be reviewed on a case-by-case basis and consideration will be given to whether the alternative standard can be mapped to an existing Operational Framework standard.

Additional supporting guidance to be included in confluence.

1c Guidance on indirect consumers and third party applications

Scope of the Operational Framework for indirect consumers (third party add-ons)

CURRENT ENVIRONMENT

DSP Operational Framework Requirements to utilise ATO digital services (pg. 4 & 5)

When a DSP provides a software product or service performs a functional role in the supply chain of transmitting Taxation or Superannuation related data through ATO digital wholesale services then that product or services is within scope of the Framework. This includes DSPs that use an intermediary (such as a gateway or sending service provider) to interact with the ATO.

WHATS NEW

The Digital Service Provider (DSP) Operational Framework (OPF) applies to any software product or service that performs a functional role in the supply chain of transmitting taxation, accounting-payroll or superannuation data through ATO digital wholesale services. This includes software products that connect:

- directly to ATO digital wholesale services
- indirectly via a sending service provider (SSP) for accounting-payroll services;
- indirectly via a gateway for superannuation services or superstream;
- indirectly via automation to other software products.

The application of the scope of the Operational Framework includes software products that are commercial software products, in-house developed software and in some instances when significant modification to software or white labelling has occurred.

1d Guidance on volume of records

Definition of "Taxation and Superannuation data" that counts toward the volume threshold for independent certification.

CURRENT ENVIRONMENT

DSP Operational Framework Requirements to utilise ATO digital services (pg. 27)

Definition for highly leveraged or high volumes of Taxpayer or Superannuation records in the glossary.

A DSP product or service that stores over 10,000 'accessible individual taxpayer or superannuation related information' records. Records that relate to the same individual are only counted once OR any gateway or SSP.

WHATS NEW

A DSP product or service that transmits over 10,000 unique client taxation, superannuation and accounting-payroll records through ATO digital wholesale services.

2 Guidance on DSP Lifecycle Management

a. Terms & Conditions relating to data breaches

b. Improvements to Letter of Confirmation

c. Improvements to Annual Review process

d. Notification of significant changes

2a Terms & Conditions relating to data breaches

Terms and Conditions

To include a timeframe and 'marketplace or ecosystems' as this information is requested in the questionnaire.

CURRENT ENVIRONMENT

Operational Framework terms and conditions

Where a breach is identified by any means e.g. monitoring, client advice, you must contact the ATO immediately to ensure appropriate action can be taken.

WHATS NEW

New language

Differentiated approach to reporting of breaches and timeframe to be reflected in terms and conditions, as per below:

- When a breach is identified within your software product or **add-on marketplace** resulting in **confirmed** fraudulent activity or identity theft you must contact the ATO within **24 hours**.
- When a breach is identified within your software product or **add-on marketplace** which **could** result in fraudulent activity or identity theft you must contact the ATO within **72 hours**.

2b Improvements to the Letter of Confirmation

Letter of Confirmation

ATO to explore options for QR code to link to the standards/requirements a DSP has met.

CURRENT ENVIRONMENT

No published content on the letter of confirmation. Supporting content is included on ato.gov.au for users of software.

WHATS NEW

Updates have been made to the letter of confirmation as per *attachment A – DRAFT letter of confirmation*, which include:

- Requirements a DSP has met based on their operating model and will include optional requirements a DSP has met.
- Business context on the requirements a product has met.

2c Improvements to Annual Review guidance and process

Annual Review process

Consider a DSP nominated period for annual review, to support each DSPs business requirements.

CURRENT ENVIRONMENT

DSP Operational Framework Requirements to utilise ATO digital services (pg. 23)

DSPs will be provided with a review date as part of their approval – typically 12 months after approval. One month prior to the review date, the DPO will remind the DSP of the review.

WHATS NEW

DSPs who have been approved under the Framework. DSPs will be provided a review date as part of their approval – typically 12 months after approval.

DSPs should contact the DPO to request an alternative date, for example to align to independent certification.

The DPO will initiate the review 6 to 8 weeks prior to the review date.

2c Improvements to Annual Review guidance and process

Annual Review process

Improved/additional guidance for uplifting to independent certification

CURRENT ENVIRONMENT

DSP Operational Framework Requirements to utilise ATO digital services (pg. 23)

DSPs will be provided with a review date as part of their approval – typically 12 months after approval. One month prior to the review date, the DPO will remind the DSP of the review.

WHATS NEW

When a DSP requires an uplift to independent certification as part of the annual review the DPO will allow a conditional period to meet certification. The DSP will need to:

- Provide the letter of engagement with external vendor,
- The project plan and timeline for completing certification process, and
- Agree to a regular check-in

2c Improvements to Annual Review guidance and process

Annual Review process

A ‘no’ changes check to save time in completing the annual review.

CURRENT PROCESS

DSPs are sent an email notification to complete their annual review. DSPs download the latest version of the questionnaire and:

1. Review prior evidence to confirm it aligns to current requirements and is up to date
2. Complete questionnaire
3. Attach evidence to questionnaire, in some cases more than what is required
4. DSPs submit their response via email back to the DPO.

WHATS NEW

The DPO created a new digital form in Online Services for DSPs. This supports a streamlined process for submitting the annual review.

Once submitted, a record of the annual review is retained within online services for DSPs.

Refer to *attachment B - Annual Review*

2d Notification of significant changes

Notification of Change

Improve guidance and requirements for notification when there is a merger or acquisition.

CURRENT ENVIRONMENT

DSP Operational Framework Requirements to utilise ATO digital services, (pg 24)

Changing circumstances

The ATO must be notified via Online Services for DSPs of any material changes to your business or product environment (i.e. relating to the information you supplied in your questionnaire response.) This may include, but not be limited to:

- change of ownership or significant Director changes
- changes in data hosting
- increase in client base (i.e. transacting greater than 10,000 unique taxation or superannuation records)
- additions or changes to DSP product or service offerings.

In this circumstance, a new Security Questionnaire may need to be provided, including updated evidence.

Note: The ATO also reserves the right to undertake ad hoc reviews to ensure DSPs maintain alignment to the requirements of the Framework.

2d Notification of significant changes

Notification of Change

Improve guidance and requirements for notification when there is a merger or acquisition.

WHATS NEW

Update the heading from “changing circumstances” to “significant changes”.

DPO must be notified in advance of significant changes.

Additional context provided around significant changes for example:

DSP Change to legal entity

- The Operational Framework terms and conditions are accepted by the legal entity and product whitelisted against the ABN of the legal entity.
- An example of a significant change to the legal entity includes mergers, acquisitions or large corporate restructures.
- Linking Operational Framework terms and conditions to significant changes.
- DSPs who engage in this process and take steps to align to Operational Framework requirements as a result of significant changes will remain approved in line with our dewhitelisting policy.
- DSPs can continue to contact us, if they are unsure if changes made are significant.

Open Discussion & Thankyou

Actions & support for working group

- Do the changes meet the overarching aim of the intent to improve information security documentation relating to updated?
- Will changes address specific outcomes relating to:
  - Supporting guidance for certification
  - Guidance and process on DSP Lifecycle Management
- Are there any other concerns or gaps we haven't been able to address?
- Closure of Requirements and Lifecycle working group?

Next steps

1. Incorporate feedback and finalise changes within the draft requirements documentation.
2. Following all smaller working groups, DPO will provide draft requirement documentation for review by the Operational Framework Review working group.