Australian Government
Australian Taxation Office

Digital Service Provider (DSP) Operational Framework Review

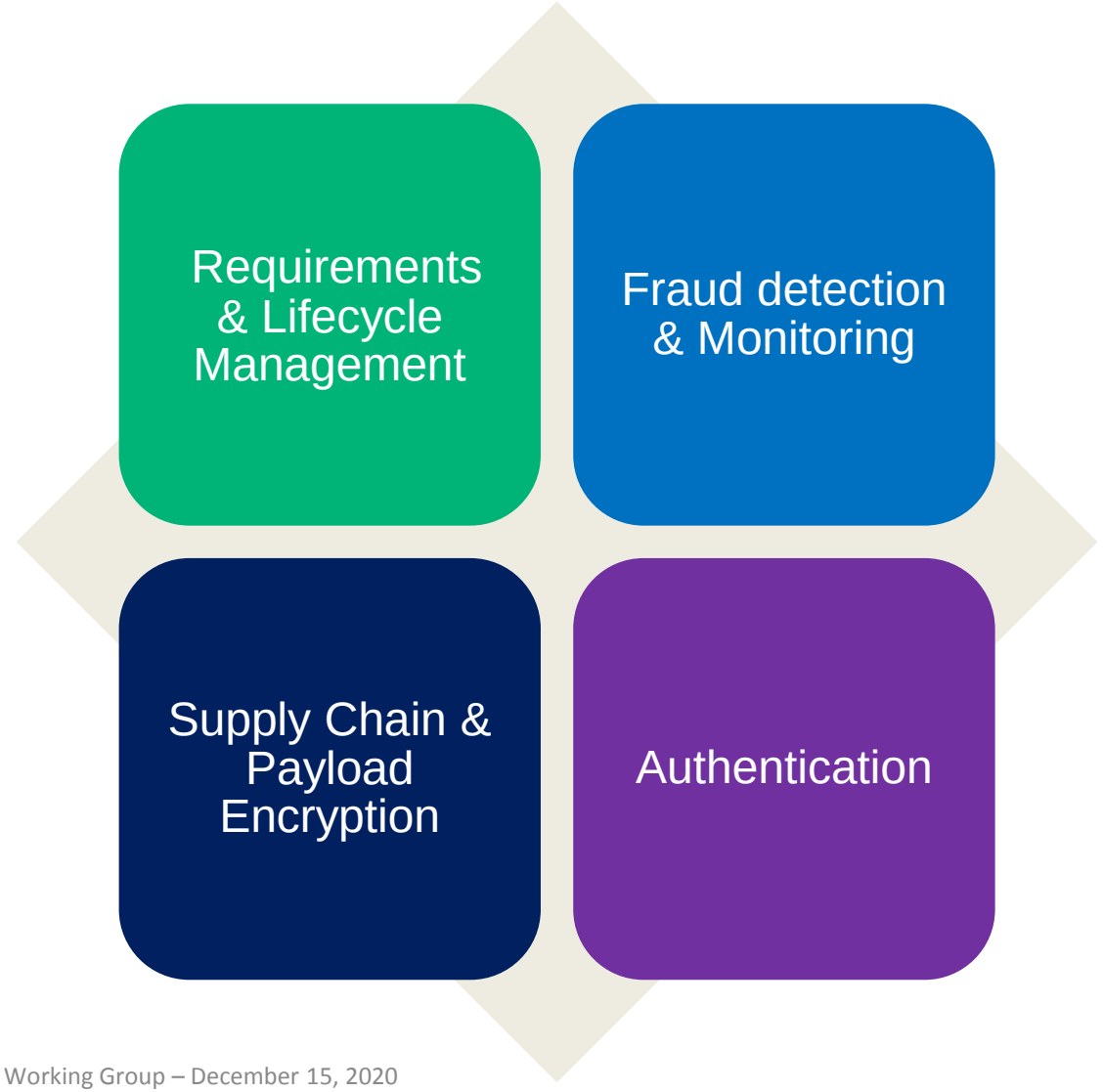
Working Group Update

Presented by Diana Porter & Kylie Johnston

15 December 2020

ATO & Industry Focus Groups

The first round of the focus groups were held with representatives across industry and ATO to foster mutually accepted outcomes, to mature the Operational Framework. The focus areas are based on independent recommendations to improve guidance or mature technical solutions.



Fraud Detection & Monitoring

- Expanding Security Monitoring Controls
- Preservation and protection of log data
- Breach Notification Guidance

Recap - What we are trying to achieve?

To improve information security documentation relating to fraud detection and monitoring controls

1 Expanding Security Monitoring

Explore benefits in expanding scope of security monitoring control to all DSP controlled cloud environments.

2 Preservation and retention of log data

Investigate and improve guidance on:

- protection and preservation of audit logs
- retention periods that align to legislative requirements.
- accessing information to share in the case of a security incident.

3 Breach notification guidance

Improve process and guidance to assist DSPs:

- Respond to breaches.
- Notify and report a security breach.
- With incident response and fraud investigations.
- With supporting information for clients.

Key outcomes from session 1 – Exploring expansion of security monitoring

Commercial impacts to be considered for smaller DSPs in expanding the control.

General sentiment on uplift of requirements to expand security monitoring it's 'good for industry'.

Sharing security information or a threat dictionary could assist DSPs in applying specific controls.

ATO should establish baseline of controls, but DSPs are best placed to determine the level.

Align security monitoring practices to business outcomes.

PROGRESS UPDATE

DPO is undertaking further analysis of feedback and is consulting with ATO SME's before changes are progressed.

The second consultation session will occur in February – March 2021 to allow additional time to work through the outcomes.

Key outcomes from session 1 – Improving protection and preservation of audit logs

Current audit logging requirements need to align the breach notification guidance.

Requirements and fields captured should be differentiated between environments e.g. SaaS vs desktop.

ATO should be more specific on expectations of log preservation.

Audit log requirements would be clearer if they were mapped to specific industry controls.

ATO should define baseline requirements and include guidance to help DSPs make risk-based decisions for audit log preservation and retention.

PROGRESS UPDATE

DPO is undertaking further analysis of feedback and is consulting with ATO SME's before changes are progressed.

The second consultation session will occur in February – March 2021 to allow additional time to work through the outcomes.

Key outcomes from session 1 - Improving breach notification guidance

A need for a mechanism for sharing information between the ATO, DSPs and third-party ecosystems when a security incident occurs.

The term “immediately” is not always practical and should align to an industry standard.

Clarity and guidance is required on risk thresholds e.g. What type of event constitutes a notification?.

Relationship between DSPs and their non-standard contractual clients around data breach notification may delay reporting and should be considered when providing guidance.

DSPs want clarity around what the ATO will do with the information provided as a result of a breach.

ATO to explore alignment of the Security for Critical Infrastructure Act 2018.

PROGRESS UPDATE

DPO is undertaking further analysis of feedback and is consulting with ATO SME’s before changes are progressed.

The second consultation session will occur in February – March 2021 to allow additional time to work through the outcomes.

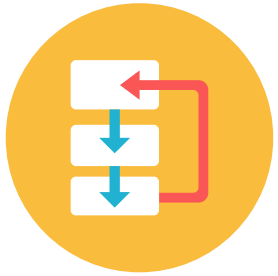
Supply Chain & Payload Encryption

- Supply Chain Visibility
- Improve Guidance for Encryption
- Explore Payload Encryption

Recap – What are we trying to achieve?

Explore opportunities to improve integrity of transactions over ATO gateways

1 Supply Chain Visibility



Explore compensating controls throughout the supply chain.

2 Improve guidance on encryption

Improve guidance for encryption in transit, at rest including key management.

3 Payload Encryption

Investigate technical solutions and adoption methodology for payload encryption.

Key outcomes from session 1 – Improving supply chain visibility

Various external systems have multiple layers or services before data is sent to the ATO.

Threat modelling is being undertaken to identify risks within supply chain.

ATO to explain the risk further rather than provide theoretical risks.

Maturity of controls within the supply chain has improved over time.

PROGRESS UPDATE

DPO is undertaking further analysis of feedback and is consulting with ATO SME's before changes are progressed.

The second consultation session will occur in February – March 2021 to allow additional time to work through the outcomes.

Key outcomes from session 1 – Exploring Payload encryption

Payload encryption suggested to be an optional requirement.

Further investigation needed on how payload encryption would be applied with the SSP model.

Payload encryption to be assessed on a risk scale against other models delivering data to the ATO.

Payload encryption options to be further explored and discussed.

PROGRESS UPDATE

DPO is undertaking further analysis of feedback and is consulting with ATO SME's before changes are progressed.

The second consultation session will occur in February – March 2021 to allow additional time to work through the outcomes.

Key outcomes from session 1 - Improving guidance for encryption

In transit
Streamline evidence requirements by DSPs providing an SSL report.
Updating TLS requirements from TLS 1.3 to TLS 1.2.

At rest
Requirements for further data encryption when the S3 bucket is already encrypted.

Encryption Key Management
Improvements to guidance relating to encryption key management.
Description and guidance for key management plan, mapping to other industry standards e.g. APRA CPS 234.

PROGRESS UPDATE

DPO is undertaking further analysis of feedback and is consulting with ATO SME's before changes are progressed.

The second consultation session will occur in February – March 2021 to allow additional time to work through the outcomes.

Requirements & Lifecycle Management

- Supporting Guidance for certification
- Guidance on DSP Lifecycle Management

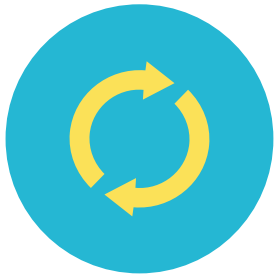
Recap – What are we trying to achieve?

Explore opportunities to improve process, guidance and documentation relating to requirements and lifecycle management of the operational framework

1 Supporting guidance for certification

Support for DSPs undertaking self certification including complementary security standards.

2 Guidance on DSP Lifecycle Management



- Terms & conditions.
- Letter of confirmation.
- Annual review process.
- Notification of DSP product environment changes.

Key outcomes from session 1 – Improving guidance for certification

Scope of certification, when it should be applied to the business and/or the product.

Definition of “tax and super data”, clarification needed if it counts toward the volume threshold for independent certification.

Clarification on definition for indirect consumers (third party add-ons) of ATO APIs, to determine if they are within scope.

Guidance should be provided around specific controls of standards applied to smaller DSPs demonstrating alignment of security posture i.e. complete ISO 27001.

PROGRESS UPDATE

DPO is undertaking further analysis of feedback and is consulting with ATO SME’s before changes are progressed.

The second consultation session will occur in February – March 2021 to allow additional time to work through the outcomes.

Guidance on DSP Lifecycle Management

- Terms and Conditions
- Letter of Confirmation
- Notification of Changes
- Annual Review Process

Key outcomes from session 1 - Guidance on DSP lifecycle management

Terms and Conditions
'Immediately' to have a value and include 'marketplace or ecosystems'.

Letter of Confirmation
ATO to explore options for QR code.

Notification of Change
Improve guidance and requirements for notification when there is a merger or acquisition.
DSPs to be notified when changes are made to published documentation in addition to the DSP newsletter.

Annual review process
Consider a DSP nominated period for annual review.
A 'no changes' check on the questionnaire.
Improved/additional guidance for changing certification requirements.

PROGRESS UPDATE

DPO is undertaking further analysis of feedback and is consulting with ATO SME's before changes are progressed.

The second consultation session will occur in February – March 2021 to allow additional time to work through the outcomes.

Authentication

- Customer Verification & Entity Validation
- Exploring Expansion of MFA
- Opportunities to Improve Guidance
- M2M Credential

Recap - What we are trying to achieve?

To identify and explore opportunities to improve authentication controls including Customer Verification & Multi Factor Authentication (MFA).

1 Customer Verification & Entity Validation

- Customer verification between DSPs and clients.
- Supporting end user clients within software.

2 Exploring the Expansion of MFA

Explore feasibility to expand MFA to all environments and users.

3 Opportunities to Improve Guidance

- 'Remember me' Functionality & Cookies.
- Single Sign-On.

4 M2M Credential

Explore feasibility to identify individual user of M2M credential.

Key outcomes from session 1 - Customer verification between DSPs and clients

No simple digital solution that links an individual to an entity.

Support for entity validation which will provide pathway to customer verification.

Exceptions to validation to be considered i.e. clients with no ABN.

Challenges in applying to desktop software.

Frequency of customer verification, initial registration, change of subscription, review process.

PROGRESS UPDATE

DPO is undertaking further analysis of feedback and is consulting with ATO SME's before changes are progressed.

The second consultation session will occur in February – March 2021 to allow additional time to work through the outcomes.

Key outcomes from session 1 - Exploring expansion of MFA

Definition of tax and super data required to assist with implementation.

Challenges and costs in implementing for desktop software.

Explore application to all users.

PROGRESS UPDATE

DPO is undertaking further analysis of feedback and is consulting with ATO SME's before changes are progressed.

The second consultation session will occur in February – March 2021 to allow additional time to work through the outcomes.

Key outcomes from session 1 - Opportunities to improve remember me functionality

Discrepancy in timeframe exists across developers.

Guidance required around use of SMS, discussion needed on security levels if used as second factor for MFA.

Timeframe impacts on user experience.

ATO to provide consistent standard on timeframe and timeouts to be applied across industry.

PROGRESS UPDATE

DPO is undertaking further analysis of feedback and is consulting with ATO SME's before changes are progressed.

The second consultation session will occur in February – March 2021 to allow additional time to work through the outcomes.

Key outcomes from session 1 - Opportunities to improve guidance for single-sign on

SSO has been supported by exception for DSPs.

Clarification around social media signing on in this context.

Definition of enterprise customer could be based on number of transactions/records.

Increased interest for SSO by tax practitioners.

PROGRESS UPDATE

DPO is undertaking further analysis of feedback and is consulting with ATO SME's before changes are progressed.

The second consultation session will occur in February – March 2021 to allow additional time to work through the outcomes.

Key outcomes from session 1 - Opportunities to improve M2M credential

Discuss opportunities to identify the individual user of M2M credential.

PROGRESS UPDATE

This item will be discussed outside of Operational Framework as it has broader Digital Identity aspects.

DPO confirmed no immediate changes are expected, the conversation was to obtain feedback from industry on the potential risks of M2M credentials including those stored on local servers where multiple client have access, potentially without MFA or user logins.

Open Discussion & Thankyou

Next steps

- Working groups February – March 2021
- DPO & ATO SME Consultation continues

Questions about Operational Framework?

Are you registered to use Online services for DSPs?
It is the best way for you to access our support. It offers a quick and simple way for you to log and track your requests with the Digital Partnership Office (DPO).

Online services for DSPs