Australian Government
Australian Taxation Office

Digital Service Provider (DSP) Operational Framework Review

Operational Framework Review Focus Group – Requirements & Lifecycle Management

Presented by Diana Porter & Jarrod Wellings

13 November 2020

What we aim 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

2 Improve guidance on encryption

A. In transit
B. At rest
C. Key management

3 Guidance and process on DSP Lifecycle Management

A. Terms & conditions
B. Letter of confirmation
C. Annual review process
D. Notification of DSP product environment changes

1 Supporting guidance for certification

The current state of certification and self-certification

The intent of certification and self-certification is for DSPs to demonstrate that they have robust security controls in place

Independent certification

Applies to DSP controlled solutions that interact with > 10,000 unique tax or super records.

Evidence requirements

ISO 27001

Independent ISO 27001 certificate and Statement of applicability.

iRAP

Independent assessors auditor report.

Self-Certification

Applies to client controlled solutions and DSP controlled solutions with < 10,000 unique tax or super records.

Evidence requirements

ISO 27001

Response to full control suite. When compliant reference policy or process. When non-compliant provide context.

iRAP

Assesses against the 900 controls of the Australian Government Information Security Manual.

Self-Certification

Applies to client controlled solutions and DSP controlled solutions with < 10,000 unique tax or super records and consuming low risk APIs.

Evidence requirements

OWASP ASVS 3.0 or OWASP ASVS 4.0

Response up to all controls up to level 2. When compliant provide details, when non-compliant provide context.

SOC2

Response to collection of control criteria on how organisations regulate their information. Includes risk management, change management, system operations, logical and physical access controls and monitoring of controls.

What benefits can improved guidance provide?

Better guidance to support DSPs meet certification and self-certification requirements

Self-certification process

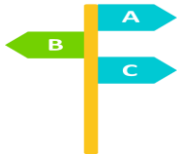
Reduced time

Less impacts to resourcing

Increased knowledge and understanding

Independent certification process

Greater alignment to global/industry standards



Greater flexibility in standards

Improve guidance on scope

Opportunities to streamline the process of certification

Other standards and framework requirements to be considered for the Operational Framework

Essential 8 ACSC Australian Cyber Security Centre

Sets baseline of mitigation strategies making it harder for adversaries to compromise systems.

Information security standards and management practices for selection, implementation and management of controls considering an organization's information security risk environment(s).

Information security standard for organisations that handle branded credit cards from the major card schemes.

GNGB GATEWAY NETWORK GOVERNANCE BODY

Sets requirements to ensure the integrity, stability and efficiency of the Superannuation Transaction Network.

NIST National Institute of Standards and Technology U.S. Department of Commerce

NIST Cyber Security Framework developed in US to protect critical infrastructure. 5 core components of the framework include to identify, protect, detect, respond and recover.

ACCC AUSTRALIAN COMPETITION & CONSUMER COMMISSION

Sets legislative security requirements in relation to consumer data rights.

What are our opportunities to streamline processes and improve guidance to DSPs to complete certification?

2 Supporting guidance for encryption

- A In Transit
- B At Rest
- C Key Management

Encryption in Transit

A Opportunities to improve documentation and to address any potential gaps

Current Encryption in Transit requirements

(Mandatory) Encryption in transit is enforced using an approved cryptographic protocol (for example, TLS 1.3) and algorithm as per the Australian Government - Guidelines for using cryptography (PDF, 1.0MB)External link (May 2019).

Evidence:
When directly connecting to the ATO provide a screenshot of one of the below:

- SSL certificates
- Showing HTTPS protocol being enforced
- Call to API
- TLS handshake protocol being enforced.

When using a SSP/Gateway to indirectly connect to the ATO provide a screenshot of one of the below:

- Licensing agreement or contract for service with SSP
- Call to the SSP REST API
- Screenshots from within SSP portal configuration page showing DSP as a linked entity
- Handshake agreement with SSP showing TLS 1.2 or HTTPS being enforced.

Opportunities to Improve framework documentation:

ACSC Australian Cyber Security Centre — **Guidelines for implementing certificates, TLS and HTTPS**

 **SSL report to streamline evidence requirements**

 **Remove support for TLS 1.0 and TLS 1.1**

FUTURE — **Plan to transition to TLS 1.3 and maintain support for 1.2**

Any concerns or feedback?

Encryption at Rest

B Seeks to protect taxation or superannuation information from unauthorised access. Applies to data repositories that manage tax or superannuation related information.

Current Encryption at Rest requirements

DSPs can chose to apply encryption at the disk, container, application or database level. Encryption at rest should follow Guidelines for using Cryptography (May 2019).

Evidence required

- Screenshot showing encryption enabled at the database or disk level with the type of encryption at rest being used
- When using 'out of the box' encryption a licensing agreement or screenshot showing 'out of the box' encryption at rest enabled
- If using the infrastructure of a cloud provider to encrypt data at rest, an invoice or contract agreement could be provided or screenshot from within the cloud environment showing encryption enabled.

Where encryption at rest is not viable, evidence must be provided of a full range of data protection controls. These must include:

- User/system (service account) access control (including authentication and authorisation) and active logging and monitoring protocols
- Intrusion Detection System/Intrusion Prevention System
- Internal employee screening or vetting
- Isolation of/and handling procedures for sensitive data including restrictions such as 'need to know' principles.

Opportunities to Improve framework documentation:

Improve existing evidence requirements

Encryption at rest support for client controlled solutions

Any concerns or feedback?

Encryption Key Management

C Seeks to minimise the risks of compromised encryption keys.

Current Encryption Key Management requirements

You need to demonstrate that a policy or process in place to govern the use of your encryption keys.

The scope of this policy should cover three categories:

- Asymmetric/public key algorithms,
- Hashing algorithms,
- Symmetric encryption algorithms.

Evidence required

Your key management plan should cover the generation, distribution, storage, access, renewal, revocation, rotation, length and complexity of keys, recovery, archiving and destruction of compromised encryption keys.

Opportunities to improve documentation

Description and guidance for a key management plan

Mapping to or referencing other industry standards such as APRA CPS 234

Any concerns or feedback?

3 Guidance on DSP Lifecycle Management

- A Terms and Conditions
- B Letter of Confirmation
- C Annual Review Process
- D Notification of Changes

Terms and Conditions

A Opportunities to discuss current terms and conditions.

Operational Framework terms and conditions

1. The ATO must be notified of any changes to your business or product environment in relation to the information you supplied in your questionnaire. Failure to do so may result in your product being de-whitelisted. The ATO reserves the right to undertake ad hoc reviews to ensure DSPs maintain alignment to the requirements of the Operational Framework.
2. Monitoring is considered a joint responsibility between the ATO and the DSP. The ATO conducts monitoring at the network, application and transaction layers. If anomalies or areas of concern are identified, we may re-assess your whitelisting suitability. The ATO will generally contact you or your representative before making changes to your whitelisted status unless exceptional circumstances apply.
3. 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.
4. In line with standard industry practice, certification (both independent and self–assessed) must be current. Where certification lapses before the review date below, you must take the appropriate steps to update and supply the ATO with a current copy of your certification.
5. There are a number of requirements that have outstanding technical solutions. For example - authentication, payload encryption and supply chain visibility. As these solutions are completed we will advise you of the further requirements for your implementation.

Any concerns or feedback?

Letter of Confirmation

B Intent of the letter of confirmation is to provide assurance that a DSP product has met the requirements of the operational framework.

Current Letter of Confirmation

Australian Government
Australian Taxation Office

DD MONTH YEAR

Letter of Confirmation

DSP Operational Framework Compliance

This letter is to confirm **Legal Entity (Product)** has demonstrated their compliance against the requirements of the Digital Service Provider (DSP) Operational Framework (the Framework).

The next review date for Product is Month Year.

The Framework is a risk scaled model that sets minimum requirements a DSP needs to meet in order to consume ATO services. The Framework reduces the risk of identity theft, fraud and system hacks and aims to protect the integrity of tax and superannuation systems.

Further details on the Framework requirements can be found at DSP Operational Framework.

If you would like to confirm the validity of this letter, please email DPO@ato.gov.au.

Regards

(NAME OF DIRECTOR)
Director
Digital Partnership Office
Australian Taxation Office

ATO | *Working for all Australians*

April 2020

ATO.gov.au website content updated in relation to the Operational Framework.

https://www.ato.gov.au/General/Online-services/ATO-digital-wholesale-services/Digital-service-provider-Operational-Framework/

June 2020

DPO updated processes in June so that all DSPs receive a letter of confirmation once they meet all the requirements of the framework and accept the terms and conditions. For existing DSPs this will be upon every annual review. Previously these were only issued on request.

January 2021

DPO are proposing to update content in the letter of confirmation to show the business model or type of requirements being met. This will support DSPs who need to provide evidence for their application of CDR to ACCC.

Any concerns or feedback?

Annual Review Process

C Opportunities to discuss and refine the annual review process.

Current Annual Review Notification

Australian Government
Australian Taxation Office

Operational Framework Annual Review
Digital Software Provider

Hi (DSP Contact),

I am writing in relation to the annual review of **DSP Name (DSP Product)** that is due to be completed by the XX th of XXXX 2020.

Since your product was approved the DSP Operational Framework has continued to evolve and change.

Next Steps

To complete the annual review:

1. Review DSP - Requirements to utilise digital services and DSP Operational Framework.
2. Confirm if there have been changes to your business or product environment.
3. Complete section 'A' of the DSP operational framework and if applicable section 'E'.
4. Confirm your evidence aligns to the current requirements and is up to date (If you previously supplied evidence with an expiry date check if it has passed).

Once completed submit a response to the annual review by raising a ticket through our Online Services for DSPs or emailing DPO@ato.gov.au.

Need help?

To ask a question or request assistance lodge a ticket through Online Services for DSPs or email DPO@ato.gov.au.

Kind Regards

Digital Partnership Office
Operational Framework Team
Australian Taxation Office

ATO | Working for all Australians

Suggested opportunities to improve the process

Improving existing OS4DSPs process

Clarity to assist DSPs understand what is required

Reducing time and complexity

Any concerns or feedback?

Notification of Changes

D Opportunities to improve documentation to address and mitigate future risks

Current requirements Notification of Changes

This is stated in the terms and conditions and examples of changes are listed in the requirements:

The ATO must be notified via Online Services for DSPs or DPO@ato.gov.au 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. 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.

Suggested opportunities to improve

Clarity on what is a change and how to notify

Timeframe to notify of change

Any concerns or feedback?

Summary & Actions

Summarised Outcomes

1. Supporting guidance for self-certification

2. Supporting guidance for Encryption
   a) In Transit
   b) At Rest
   c) Key Management

3. Guidance on DSP Lifecycle Management
   a) Terms & Conditions
   b) Letter of Confirmation
   c) Annual Review Process
   d) Notification of Changes