Australian Government
Australian Taxation Office

Operational Framework for Digital Service Providers

Implementation Approach

February 2018

Version 1.0

For more information on this paper, email DPO@ato.gov.au

Contents

What is the Digital Service Provider Operational Framework?

The Operational Framework aims to strengthen the security of the digital taxation and superannuation ecosystem. By establishing a level of confidence and certainty, the ATO will be able to continue to invest in and extend the services made available through our digital wholesale channels.

Securing the ecosystem will also provide increased levels of confidence to tax professionals, businesses and individuals. The ATO will additionally publish each Digital Service Providers (DSPs) high level conformance outcomes, enabling full transparency and increased levels of comfort for potential and existing users.

Through the implementation of ATO Application Programming Interface APIs and services, Digital Service Providers (DSPs) make a range of taxation and superannuation related services available to the community. The ATO recognises the strategic importance of this service delivery channel, and is at the forefront of API exposure; being significantly more advanced than other revenue agencies.

The ATO acknowledges the inherent risks of exposing API services and sensitive information externally. The Digital Service Provider (DSP) Operational Framework (Framework) is part of the ATO response in recognising and responding to these risks. The Framework has also been developed in line with the Tax File Number Rule of the Privacy Act 1988 (sections 10, 11) and Division 355 - Confidentiality of taxpayer information in the Taxation Administration Act 1953.

The DSP Operational Framework requirements and implementation approach has been developed through a consultation process involving the Digital Business Council (DBC), Australian Business Software Industry Association (ABSIA), Gateway Network Governance Body (GNGB) and many Digital Service Providers (DSPs).

Intent

The DSP Operational Framework seeks to protect tax or superannuation related information as well as the integrity of the tax and superannuation systems which support the Australian community. Specifically the framework is a response to:

- Information gain – including identity theft, personal gain or commercial advantage.
- Financial gain – including tax refund fraud
- Destructive behaviour – including individual or system hacks

Who is covered by the framework

If a Digital Service Provider (DSP) provides a software product or service that reads, modifies or routes any tax or superannuation related information, then that DSP is in scope of the DSP Operational Framework. This includes DSPs that use an intermediary, such as a gateway or sending service provider to interact with the ATO systems.

Provision of a software product or service, includes:

- commercial software,
- non-commercial (freeware) or
- in house developed products, that are used to manage the tax or superannuation affairs of other entities or individuals

Note that products or services that provide supplementary services that are not tax or superannuation related (e.g. most 3rd party add on providers to accounting platforms), are not in scope of the framework.

DSPs that are already using our services are required to transition to these requirements over time.

Examples

- Desktop accounting product sold commercially - IN scope
- Freeware payroll product - IN scope
- Sending Service Provider - IN scope
- Cloud based accounting platform - IN scope
- Payroll bureau using in house developed software - IN scope
- Payroll system developed in house by an organisation for the purpose of managing their own affairs – NOT IN scope
- Document management system that plugs into accounting platform - NOT IN scope

Objectives of the framework

The DSP Operational Framework has five objectives that provide the foundation for a thriving and robust digital ecosystem.

The integrity and reputation of the ecosystem is protected by the controls that are implemented and adhered to by all of its participants.

The ATO on its own cannot maintain the integrity and reputation of the ecosystem. All participants have responsibility for the ongoing protection of the digital ecosystem.

The requirements to use our services are dependent on the level of risk presented.

The framework seeks to establish a risk based approach to the level of controls that are implemented by DSPs. Some DSPs will only consume simple, low risk services, some DSPs will only produce desktop software, while some DSPs may provide cloud services which are wholly hosted in ASD certified environments. Expectations are customised based on risk level.

Conformance with the DSP Operational Framework is an ongoing expectation.

Continued entitlement to participate in the ecosystem is dependent on continuing to meet the requirements. Regular reviews to ensure continued conformance is necessary.

The DSP Operational Framework matures and evolves over time to accommodate the shifting opportunities and risks of the ecosystem.

> The framework does not have an end date, continuous advancements in technology will mean the DSP Operational Framework needs to have a capability to grow over time and adapt to combat emerging risks or take advantage of new opportunities.

The DSP Operational Framework can be adapted across the broader ecosystem, including other agencies and commercial organisations

> Any solution implemented would be customisable, flexible and could be applied across the whole of government, and commercial organisations such as banks.

What are the Requirements

The framework utilises a differentiated risk model in determining the requirements needed for utilising ATO's APIs. Factors include the API risk rating, volume of accessible individual taxpayer or superannuation records, along with a number of elements of the DSPs operating model (e.g. on premise or cloud based software, data hosting arrangements and if there is an intermediary within the supply chain to the ATO).

Requirements for products and or services hosted by the client

This includes desktop software or software hosted by the client on premise, or within either an Infrastructure as a Service (IaaS) or Platform as a Service (PaaS) environment.

Requirements	**Connects directly to the ATO**	**Connects indirectly to the ATO (e.g. via gateway or SSP)**
Personnel security	(Mandatory) A personnel security integrity check process should be in place.	
Encryption in transit	(Mandatory) Encryption in transit is mandatory using [ASD approved cryptographic algorithms and protocols] (for example, TLS 1.2)	
Encryption at rest	(Optional)	
Payload Encryption	Not applicable	(Mandatory where supply chain visibility is not implemented) Payload encryption solution is not currently available, but will be developed in the near future. The solution will be based on Cryptographic Message Syntax (CMS).
Encryption key management	(Mandatory) Encryption key management (including Public Key Infrastructure (PKI) keys) complies with [ASD / industry guidelines (see p.g. 259-262)]	
Audit logging	(Mandatory) Appropriate audit logging functionality implemented	
Product ID in message header	(Mandatory) The Product ID of the software that produces the payload information must be included in the message.	
Certification	(Mandatory) Self-assessment against either: • iRAP • ISO / IEC 27001 • OWASP ASVS3.0 or • SOC2	
Supply chain visibility	Not applicable	(Mandatory) The supply chain visibility solution is not currently available, but will be developed in the near future.
Data hosting	Not applicable	
Authentication	(Optional) Multifactor authentication	(Optional) Multifactor authentication
Security monitoring practices	(Mandatory) DSPs that utilise web services (e.g. hybrid desktop environments) are required to have security monitoring in place. For example: • Network / infrastructure layer • Application layer • Transaction (data) layer	

Note: DSP products and or services hosted by the client that use web services (e.g. hybrid desktop products), will be assessed on a case by case basis and may require different requirements to address differences in the risk profile.

Requirements for products and or services hosted by the DSP

This includes Software as a Services (SaaS), gateways and sending service providers.

Requirements	Low volumes of taxpayer or superannuation records (<10k)		Highly leveraged or high volumes of taxpayer or superannuation records (>10k)[1]
	Consumes no / low risk APIs only	Consumes medium or high risk APIs	-
Personnel security	(Mandatory) A personnel security integrity check process should be in place.		
Encryption in transit	(Mandatory) Encryption in transit is mandatory using ASD approved cryptographic algorithms and protocols (for example, TLS 1.2)		
Encryption at rest	(Mandatory) Encryption at rest is mandatory using ASD approved cryptographic algorithms and protocols. Examples may include; full-disk, container, application or database level encryption techniques.		
Payload encryption Applicable when the product or service does not connect directly to the ATO and the Supply chain visibility functionality is not available	(Mandatory) Payload encryption solution is not currently available, but will be developed in the near future. The solution will be based on Cryptographic Message Syntax (CMS)		
Encryption key management	(Mandatory) Encryption key management (including PKI keys) complies with ASD / industry guidelines (see pg 259-262)		
Audit logging	(Mandatory) Appropriate audit logging functionality implemented		
Product ID in message header	(Mandatory) The Product ID of the software that produces the payload information must be included in the message.		
Certification	(Mandatory) Self-assessment against either: • iRAP • ISO / IEC 27001 • OWASP ASVS3.0or • SOC2	(Mandatory) Self-assessment against either: • iRAP or ISO / IEC 27001	(Mandatory) Independent assessment against either: • iRAP or • ISO / IEC 27001
Supply chain visibility Applicable when the product or service does not connect directly to the ATO and the payload encryption is not used	(Mandatory*) The supply chain visibility solution is not currently available, but will be developed in the near future. * Mandatory if product or service does not connect directly and payload encryption is not used.		
Data hosting	(Mandatory) Data hosting on shore by default. Offshore hosting arrangements (including redundant systems) are managed by exception only.		

[1] Refer to Glossary for definitions

Authentication	(Mandatory) Multifactor authentication	
Security monitoring practices	Not applicable	(Mandatory) Security monitoring is in place. For example: • Network / infrastructure layer • Application layer • Transaction (data) layer

Additional Requirement Information

Certification and Assessment

To provide the ATO with a level of assurance that DSPs have robust security practices in place, the ATO has drawn on government and industry best practice to determine DSP certification requirements.

DSPs able to successfully attain certification and contextualise non-compliances identified as part of the certification exercise will support the ATO and the Australian Community to manage the emerging cyber threats associated with exposing taxpayer data.

Certification requirements are relevant to the service model used by the DSP, number of individual taxpayer records that are read, routed or modified and the risk rating of the services used.

The ATO has assessed the following security standards for DSPs to provide assurance:

- iRAP
- ISO / IEC 27001
- OWASP ASVS3.0 or
- SOC2

DSPs are able to request to use an alternative security standard if they feel it would be more suitable for their circumstances. These requests will be assessed on a case-by-case basis.

Payload Encryption

Payload encryption can be used to provide end-to-end protection for sensitive or classified information. Payload encryption is the preferred solution for transporting sensitive or classified information through a supply chain. DSPs must, at a minimum, implement either payload encryption or supply chain visibility requirements.

Supply Chain Visibility

When information is sent from one party to another (e.g. from a taxpayer to the ATO), the data can be sent through a number of different parties in a ‘supply chain’. Each party in the supply chain can perform one or more functional roles.

The below design principles and functional roles will inform the development of a future technology solution to deliver supply chain visibility.

Supply Chain Visibility involves annotating the identity and functional role to the message for every DSP that reads or modifies the data – where the payload is not encrypted end-to-end (i.e. payload-level encryption).

Where payload encryption has been implemented supply chain visibility is not required.

Design Principles

1. The technical solution will seek to balance the need for risk mitigation against need for operational effectiveness.
2. If a DSP reads or modifies any data, the message must be annotated with that DSP's identity and functional role(s) in the supply chain.
3. DSPs are not responsible for information after it has been securely delivered to an authenticated and authorised customer.
4. If a DSP routes a message, the message must be annotated with that DSP's Identity and functional role for operational support reasons.

Functional Roles within a Supply Chain

The functional roles within a supply chain are defined as:

- **Data Collector**: Party responsible for the acquisition of data through user interface interaction or APIs
- **Data Validator**: Party responsible for the verification of data types, structures, formats andor data values
- **Data Integrator**: Party responsible for combining data from multiple sources for use
- **Data Analysis and Extraction**: Party responsible for performing analysis on data to extract a data sub-set or additional derived/calculated data
- **Data Transformer**: Party responsible for change syntactic representation of data
- **Data Provider**: Party responsible for the payload (which maybe encrypted)
- **Data Transmitter**: Party responsible for the message with the payload. (e.g.. ebMS3/AS4 transmission)

Onshore/Offshore Data Hosting

Storing data in a foreign jurisdiction presents additional risks that must be considered.

Requirements

1. Consistent with guidelines for Australian, Prudential Regulation Authority (APRA) -regulated entities, the ATO expects DSPs to apply a cautious and measured approach when considering retaining data outside the jurisdiction it pertains to.
   By default, the ATO expects DSPs to store data onshore.

2. **Where there is a compelling reason for storing data outside of Australia a DSP must consult with the ATO prior to entering into any offshore data hosting arrangement** so that the ATO may satisfy itself that the impact has been adequately addressed.
   As part of the consultation:
   a. DSPs must demonstrate they have considered the jurisdictional risks of storing data in a foreign jurisdiction.
   b. The ATO can provide advice on jurisdictional constraints.

   The ATO will consider requests to host data offshore on a case by case basis.

3. The ATO's preference is for all redundancy hosting locations to mirror those of the primary production environment. With strong encryption controls and alignment to the APRA guides CPG 235-Managing Data Risk and SPG 231-Outsourcing, DSPs may consult with the ATO on the suitability of redundancy hosting arrangements in an offshore location with redundancy hosting reviewed upon a case by case circumstance.

Additional conditions for offshore data hosting

1. Consistent with APRA's Cross Industry Prudential Practice Guide CPG 235- Managing Data Risk, the ATO expect the following would normally be applied to the assessment and ongoing management of offshore data hosting:

   - Enterprise frameworks such as security, project management, system development, outsourcing/offshoring management and risk management,
   - A detailed risk assessment,
   - A detailed understanding of the extent and nature of the business processes and the sensitivity/criticality of the data impacted by the arrangement,
   - A business case justifying the additional risk exposures.

2. Consistent with APRA's Prudential Standard Guide SPG 231-Outsourcing, the ATO expects that DSPs would address the following specific risks and any other identified risks by:

   - **Country risk**: the risk that overseas economic, political and or social events will have an impact upon the ability of an overseas service provider to continue to provide an outsourced service to the DSP,

- **Compliance (legal) risk:** the risk that offshoring arrangements will have an impact upon DSP's ability to comply with relevant Australian and foreign laws and regulations (including accounting practices),
- **Contractual risk:** the risk that a DSP's ability to enforce the offshoring agreement may be limited or completely negated,
- **Access risk**: the risk that the ability of a DSP to obtain information and to retain records is partly or completely hindered. This risk also refers to the potential difficulties or inability of the ATO to gain access to information using ATO information gathering powers, and
- **Counterparty risk:** the risk arising from the counterparty's failure to meet the terms of any agreement with the DSP or to otherwise perform as agreed.
- The ATO expects that an offshoring arrangement would typically include a provision around security and confidentiality of information.

3. Where you are storing data outside of Australia you must:
    - Make it clear to your customers that their data is being stored in a foreign jurisdiction,
    - Apply the Australian Privacy Principles,
    - Provide guidelines to your customers, where your customers use your services to collect and store data about other individuals (eg clients of tax practitioners, employees, etc.), on where and how their data is being managed.

Identity and Authentication

Requirements

1. Subject to the design and delivery of the Trusted Digital Identity Framework (TDIF) DSPs will be required to either:
    a. Use the current Cloud Authentication and Authorisation (CAA) solution with the addition of a multi-factor credential.
    b. Consume the government provided TDIF credential, or
    c. Become a TDIF credential provider in their own right and consume their own credential.
2. In the interim, whilst the TDIF standards and solutions are being developed for use in software products, DSPs must:
    a. Review their security credential risks and develop a plan to manage identified risks, and
    b. Implement and mandate a multifactor credential solution for all users with access to taxation or superannuation related information or provide assurances that sufficient controls are in place to mitigate the risks.

Multi-factor authentication (MFA)

Access to systems and the information they process, store or communicate need to be controlled through strong user identification and authentication practices. Multi-factor authentication uses independent means of evidence to assure a user's identity.

The three authentication factors are:

- Something one knows, such as a passphrase or a response to a security question,
- Something one has, such as a passport, physical token or an identity card,
- Something one is, such as biometric data, like a fingerprint or face geometry.

Any two of these authentication factors must be used to achieve multi-factor authentication. If something one knows, such as the passphrase, is written down or typed into a file and stored in plain text, this evidence becomes something that one has and can defeat the purpose of multi-factor authentication.

Trusted Digital Identity Framework (TDIF) credentials will provide multifactor authentication.

Many DSP products and or services perform tasks outside of the tax and superannuation space. User accounts that do not have access to taxpayer or superannuation related information are not required to meet the above requirements.

Audit logging standards

We appreciate each DSP's system is architected differently with limited universal design components. Standards for audit logging are therefore not in a prescriptive format – but rather based on a number of key components. DSPs should consider their environment and what logging should be implemented and ensure that the logging records include the following details where applicable: Date and time of the event

- Relevant users or process (i.e. who, user account and random number RAN)
- Event description
- Success or failure of the event
- Event source e.g. application name
- ICT equipment location and identification
- Data identifiers (product ID, Tax File Number (TFN)

Note:

- Along with audit log data, we will also require a data dictionary that aligns the data attributes to key components
- Audit logs will need to be exportable in flat CSV formats

Event log auditing for Gateways

Gateway Operators must develop, document and implement event log auditing requirements covering:

- The scope of audits
- The audit schedule
- What constitutes a violation of information security policy
- Action to be taken when violations are detected
- Reporting requirements
- Specific responsibilities

Personnel Security Procedures

Personnel Security Procedures are required to be in place for all DSPs. It is expected that DSPs can evidence this by providing internal policy documents - including descriptions of the process.

Personnel security procedures may include a variety of measures including but not limited to:

- Identity proofing
- Qualification checks
- Previous employment checks
- Criminal records check / police check
- Employee obligations
- Separation activities

Note: DSPs that are micro-businesses (one or two employees) may not require personnel security procedures unless contractors or non-employees have access to source code or tax or superannuation related information.

Product ID

The Product ID of the system that generates the original payload information (e.g. payroll or accounting system) for submission to the ATO rather than the intermediary (e.g. Sending Service Provider) that sends the ebms3 message to the ATO must be included in the message header. Exceptions apply in the SuperStream environment.

Minimum evidence requirements

As part of the Product Review Questionnaire, DSPs need to provide suitable evidence of how their product or service meets the relevant requirements. Examples of suitable evidence include:

Authentication

- Published product description
- User manual, user description, user instructions paired with screen shots of the user interface

Encryption

Relevant combinations of:

- Screen shots (of the configuration page),
- Configuration files,
- Product data sheet/white papers (together with Product purchase/ownership documentation such as receipts, front page of a contract of product/support/service),
- Federal Information Processing Standard Validation documents (US government computer security standard, e.g. FIPS 140-2),
- Product Common Criteria Evaluation documents, or
- Product Evaluation Assurance Level (EAL) documents

Certification

- iRAP letter of compliance or iRAP assessor engagement details,
- ISO27001 documentation and Certificate of Compliance / Registration or Statement of Applicability with Certificate of Compliance, or
- Evidence of OWASP ASVS3.0 or SOC2 assessment

Data hosting

- Name of ASD certified data hosting provider, or
- Data hosting providers details, including:
  - Provider name,
  - provider location (onshore / offshore),
  - redundancy location
  - If data is stored offshore further evidence is required. See *Additional conditions for offshore data hosting* below for more information.

Personnel security

- Internal policy document, and
- Process description

Encryption key management

- Key Management Plan (internal documentation)

Security monitoring practices

- Network / Infrastructure layer examples
  Relevant combinations of:
  - Screen shots (product page, the management console page)
  - Product purchase/ownership doco (e.g. receipts, front page of a contract of product/support/service)
  - Configuration files
  - Photos of the product
  - Photos of SOC/SIEM centre (using the products)

- Application Layer example
  - Screen shots of the function page in the application, and
  - Reports from the backend system

- Transaction (data) layer example
  - Reports from the backend system
  - Previous unusual cases

Audit logging

- Data dictionary that describes the data attributes and maps against key audit log components
- Sample of dummy audit log in CSV format

Implementation

The DSP Operational Framework introduces a number of requirements that DSPs will be required to meet. The ATO recognises that it will take time for DSPs to meet the requirements. In addition, it will also take time for the ATO to adequately assess the evidence that DSPs provide.

To cater for this each requirement has a different commencement date. There is also a transition strategy to slowly transition DSPs into the Operational Framework. Whilst DSPs will be provided time to transition, planning should be done early to ensure they are able to meet the timeframes.

When does each requirement come into effect?

Certification and Assessment

It is recognised the certification process can take time depending on the standard chosen and the maturity of the organisation. The ATO expects most DSPs will be able to complete the process in 3-6 months however longer timeframes will be required for some. The ATO will work with DSPs on an individual basis to determine an appropriate timeframe.

- Existing DSPs will need to commence the process by **01 February 2018**.
- New DSPs will need to commence the process before they are granted access to any ATO service.

Access to new services while a DSP is progressing through the certification process will be assessed on a case-by-case basis. Evidence of commitment to undergo certification and satisfactory responses to the security questionnaire will form the basis for this assessment.

Existing DSPs will be able to access ‘like for like’ services while transitioning to the DSP Operational Framework requirements.

Encryption in Transit

- Existing DSPs will be required to implement encryption of data in transit by **01 February 2018**.
- New DSPs will need to commence the process before they are granted access to any service.

Encryption at Rest

- DSPs will be required to implement encryption of data at rest change by **01 February 2018.**
- New DSPs will need to commence the process before they are granted access to any service.

Payload Encryption

- Design for the payload encryption solution will be completed through 2018.

Implementing this change requires significant design, development and consultation efforts across industry. Consultation with industry will occur before this requirement comes into effect.

Supply Chain Visibility

- Design for the supply chain visibility solution will be completed through 2018.

Implementing this change requires significant design, development and consultation efforts across industry. Consultation with industry will occur before this requirement comes into effect.

Onshore/Offshore Data Hosting

- Existing DSPs who store data outside of Australia must notify the ATO and provide evidence of how they meet the requirements and additional conditions by **1 February 2018.**
- New DSPs who store data outside of Australia must notify the ATO and provide evidence of how they meet the requirements and additional conditions before they are granted access to any service.

Where a DSP is unable to meet the requirements and or principles the DSP will be expected to transition data to Australia within a reasonable timeframe.

Identity and Authentication

- Design and delivery timelines for the Trusted Digital Identify Framework (TDIF) are yet to be finalised.

DSPs should take a risk based approach to the implementation timeframe for multifactor authentication across their suite of products and or services. Tax practitioner products and services generally present a higher risk and as such, DSPs must implement multifactor credentials within these products and services by **31 March 2018** and mandate their use by **30 June 2018**.

For products and services where users potentially have access to large volumes of taxpayer or superannuation related information (e.g. payroll) DSPs must implement multifactor credentials by **30 June 2018** and mandate their use by **30 September 2018**.

For all other products and services hosted by the DSP, DSPs must implement multifactor credentials by **30 September 2018** and mandate their use by **31 December 2018**.

Access to value-added services may be restricted until multifactor credentials have been implemented and mandated.

Audit Logging

- All new products and or services will be required to include audit logging capability
- Transition for existing products and or services will be discussed on an individual basis with DSPs.

- It is expected that all products and or services will have audit logging capabilities in place by **01 July 2018.**

Product Identifier in message

- All DSPs are required to have the software and or product identifier in the message header effective immediately.

Personnel Security Procedures

- All DSPs are required to have in place personnel security measure effective immediately.

Transition Strategy

The transition strategy assists to identify the priority and order by which existing DSPs will move to the enduring registration and certification process under the DSP Operational Framework.

Staged Approval Process

The process of being approved under the DSP Operational Framework will be done in the following stages;

All **new** DSPs will need to seek approval under the DSP Operational Framework before consuming an API or web service.

All existing DSPs wishing to consume:

1. A new service will be expected to be approved **before** consuming the new service.
2. Practitioner Lodgement Service (PLS) services will be expected to commence the approval process by **01 March 2018.**
3. Single Touch Payroll (STP) services will be expected to commence the approval process by **01 April 2018**.
4. Taxation related services will be expected to commence the approval process by **01 May 2018**.
5. Superannuation related services will be expected to commence the approval process by **01 June 2018**.
6. Any other DSP that does not fall into the prior categories will be expected to commence the approval process by **01 Jul 2018.**

DSPs will be able to continue to access 'like for like' services during the transition period, even without meeting all the requirements under the DSP Operational Framework. Later versions of the same service (e.g. 2018 Individual Income Tax Return (IITR) service compared to 2017 IITR service) are not considered to be new services for the purpose of this transition strategy.

What happens if I can't meet the timeframes above?

We recognise that each DSP is different and the suite of products and services can be complex. Where you are unable to meet the timeframes above you should make contact with the ATO as soon as possible to discuss your situation. We will aim to work with you on an individual basis to develop a tailored transition approach that is mutually acceptable, taking into consideration your individual circumstances. However, this approach should not be used to gain a commercial advantage.

Operational Framework Approval Process

The requirements and timeframes outlined within this document are expected to be met by all DSPs seeking approval under the DSP Operational Framework.

The approval process involves a DSP completing a security questionnaire and providing relevant evidence. Once all the relevant information has been provided the ATO will assess the evidence provided and either:

- Grant approval
- Grant conditional approval
- Reject the application

Note: Where an application has been rejected for any reason and you wish to lodge an objection please contact the DPO mailbox DPO@ato.gov.au

Conditional Approval

Conditional approval may be granted in situations where the DSP is undertaking necessary steps to meet the DSP Operational Framework requirements but do not yet meet those requirements (eg undertaking certification against ISO 27001). A review date will be set when conditional approval is granted. At this time progress will be assessed and a determination made as to whether the conditional approval will continue or the DSP's access will be suspended until such time as they meet the requirements.

Changing circumstances and annual re-assessment

The ATO must be notified via your Account Manager of any material changes to your business or product environment, in relation 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

An updated security questionnaire and review of certification (independent and self-assessed) are required annually – with evidence the review provided to the ATO. The questionnaire and certification updates should reflect any material changes.

Note: The annual re-assessment process is separate from Production Verification Testing (PVT). DSPs wishing to consume services that are not like-for-like should consider the potential impact to requirements under the framework.

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

Monitoring and information incidents

Monitoring is considered a joint responsibility between the ATO and DSPs. 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. This may include increasing the requirements that you need to meet or introducing additional requirements. The ATO will generally contact you or your representative unless exceptional circumstances apply.

Where you identify a breach through your own monitoring controls you must notify the ATO immediately via your Account manager or the DPO mailbox, DPO@ato.gov.au to ensure appropriate action can be taken.

In notifying the ATO, we would request the following type of information:

- The identity and contact details of the organisation
- A description of the data breach
- The kinds of information concerned and
- Recommendations about the steps individuals should take in response.

The ATO will work with the DSP to minimise the impact on Taxpayers.

Notifiable Data Breaches

DSPs need to be aware of The Notifiable Data Breaches (NDB) scheme under Part IIIC of the *Privacy Act 1988* (Privacy Act) that establishes requirements for entities in responding to data breaches. Entities have data breach notification obligations when a data breach is likely to result in serious harm to any individuals whose personal information is involved in the breach.

For further information on the Notifiable Data Breach scheme, please refer to https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme

What happens if I don’t meet these requirements?

The ATO expects all DSPs will meet and maintain the relevant requirements of the DSP Operational Framework.

The ATO will endeavour to work through non-conformance issues with DSPs, however failure to address these issues will result in restriction of access to services or de-whitelisting. The SBR Conditions of Use enables the ATO to lawfully suspend or terminate any software product, report or information from access to the SBR channel.

The ATO is committed to the protection of tax and superannuation information and will treat issues of non-conformance seriously.

Questions

Should you have any questions in relation to this document or your requirements as a DSP, please contact the DPO mailbox directly and a member of our team will be in contact with you at DPO@ato.gov.au

Summary of Key Dates

Certification and Assessment • Existing DSP's will need to commence the process by **1 February 2018** • New DSP's will need to commence the process before they are granted access to any ATO service
Encryption in Transit • Existing DPS will be required to implement encryption of data in transit by **1 February 2018** • New DSP's will need to commence the process before they are granted access to any ATO service
Encryption at Rest • DSP's will be required to implement encryption of data at rest change by **1 February 2018** • New DSP's will need to commence the process before they are granted access to any ATO service
Payload Encryption • Design for the payload encryption solutions will be completed through 2018
Supply Chain Visibility • Design for the supply chain visibility solution will be completed through 2018
On Shore / Off Shore Data Hosting • Existing DSP's who store data outside of Australia must notify the ATO and provide evidence of how they meet the requirements and additional conditions by **1 February 2018** • New DSPs who store data outside of Australia must notify the ATO and provide evidence of how they meet the requirements and additional conditions before they are granted access to any service.
Identity, Authentication and Authorisation Management (IAAM) • Tax Practitioner products and services generally present a higher risk and as such DPS's must implement multifactor credentials within products and services by **31 March 2018** and mandate their use by **30 June 2018** • For products and services where users have access to large volumes of taxpayer data or superannuation related information e.g. payroll DSP's must implement multifactor credentials by **30 June 2018** and mandate their use by **30 September 2018** • For all other products and services hosted by the DSP, DPS's must implement multifactor credentials by **30 September 2018** and mandate their use by **31 December 2018**
Audit Logging • All new products and or services will be required to include audit logging capability • Transition for existing products and or services will be discussed on an individual basis with DSPs. • It is expected that all products and or services will have audit logging capabilities in place by **01 July 2018**
Software identifier in Message • All DSPs are required to have the software and or product identifier in the message header effective immediately
Personnel Security Procedures • All DSPs are required to have in place personnel security measure effective immediately

Transition Strategy
- All **new** DSPs will need to seek approval under the DSP Operational Framework before consuming an API or web service.   - All existing DSPs wishing to consume: - A new service will be expected to be approved **before** consuming the new service   - Practitioner Lodgement Service (PLS) services will be expected to commence the approval process by **01 March 2018**   - Single Touch Payroll (STP) services will be expected to commence the approval process by **01 April 2018**   - Taxation related services will be expected to commence the approval process by **01 May 2018**   - Superannuation related services will be expected to commence the approval process by **01 June 2018**   - Any other DSP that does not fall into the prior categories will be expected to commence the approval process by **01 Jul 2018**   DSPs will be able to continue to access 'like for like' services during the transition period, even without meeting all the requirements under the DSP Operational Framework. Later versions of the same service (e.g. 2018 Individual Income Tax Return (IITR) service compared to 2017 IITR service) are not considered to be new services for the purpose of this transition strategy.

Glossary

Term	Definition
Accessible	Information that is readily available and easily obtained by the end user.
Application programming interface (API)	An API is a set of subroutine definitions, protocols and tools for building application software.
Application Security Verification Standard (ASVS 3.0)	A framework of security requirements and controls that focus on normalising the functional and non-functional security controls required when designing, developing and testing modern web applications.
ASD approved cryptographic algorithms	Algorithms which have been extensively scrutinised by industry and academic communities in a practical and theoretical setting and have not been found to be susceptible to any feasible attack.
Australian Signals Directorate (ASD)	The ASD produces the Australian Government Information Security Manual (ISM). The manual is the standard which governs the security of government ICT systems. It complements the Protective Security Policy Framework (PSPF).
Cloud Software	Software that is delivered, stores data and is managed remotely from its users or their technology infrastructure. For example Software as a Service(SaaS).
Cryptographic Message Syntax	A process used to provide encryption and digital signature capabilities to any form of digital data.
Data at rest	Data which is in storage and is not actively moving from device to device or network to network.
Data in transit	Data that is actively moving from one location to another for instance device to device or network to network.
De-whitelisting	The process of preventing the ability to transact with ATO production services.
Digital Service Provider (DSP)	Software or solution providers that produce digital systems that perform any function within any digital supply chain handling tax payer or superannuation data.
Direct to ATO, product hosted on customer's premise or on customer's IaaS/PaaS Cloud	Software that is loaded and stored on a client's local computer, service (IaaS/PaaS) and or device and transmits direct to the ATO.
DSP service is running in the cloud	Software that has been developed to run in a cloud environment. Cloud offers the option to provide a software-as-a-service offering direct to end users or provide a software-as-a-service offering to another DSP to consume as part of a supply chain.
ebMS3	A set of layered extensions to the SOAP protocol, providing security and reliability features enabling e-Commerce transactions. ATO is using the eBMS 3 standard with the addition of the AS4 profile.

Term	Definition
Encryption	The process of encoding information in such a way that only the person (or computer) with the 'key' can decode it.
Gateway	A digital service provider that facilitates the transfer of compliant electronic data messages.
Highly leveraged or high volumes of taxpayer or superannuation records	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 sending service provider.
Indirect to ATO, product hosted on customer's premise or on customer's IaaS/PaaS Cloud via gateway	Software that is loaded and stored on a client's local computer, service (IaaS/PaaS) and or device and uses a gateway or sending service provider to facilitate the transmission of a message to the ATO.
Taxpayer or superannuation related information	Information that has been stored for the purpose of a taxation or superannuation law and identifies, or is reasonably capable of being used to identify an individual or other entity.
The Information Security Registered Assessors Program (IRAP)	An ASD initiative to provide high-quality information and communications technology (ICT) services to government in support of Australia's security. IRAP provides the framework to endorse individuals from the private and public sectors to provide cyber security assessment services to Australian governments.
ISO/IEC 27001	A family of standards which assist the ATO in managing the security of assets such as financial information, intellectual property or information entrusted by third parties. ISO/IEC 27001 is recognised as the international standard for managing information security.
Large/high leverage user base	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. Any gateway or sending service provider.
Like for Like services	A service which contains the same functionality, quality and value as one that was previously created.
Mandatory (requirement)	Requirement must be in place (or towards being implemented) before ATO services can be used in production.
Optional (requirement)	Requirement does not have to be in place to access ATO services in production.
Sending service provider	See Gateway
Service Organization	An audit report which covers operational control systems following.

Term	Definition
Control (SOC)2	Predefined criteria around security, availability, process integrity, privacy and confidentiality.
Trusted Digital Identity Framework (TDIF)	A framework which provides the policies and guidelines that will govern delivery of the digital identity solution
Whitelisting	The process of gaining access to transact with ATO production services.

Document Details

Attributes	Details
Date Produced	Draft Issued 19December 2017 Final Issued 08 February 2018
Date Latest Release	08 February 2018
Document Name	Operational Framework for Digital Service Providers Implementation Approach
Document Creators	Martin Mane, Diana Semetas, Terry Seiver
Distribution	DSP External Community ATO Internal Community
File Location	Software Developers Website https://softwaredevelopers.ato.gov.au/

Version History

Version	Date	Changes	Date Rectified	Date Released
0.1	December 2017	Document creation and draft released	December 2017	December 2017
1.0	08/02/2018	Finalised Version Released	08/02/2018	08/02/2018