Australian Government
Australian Taxation Office

Digital service provider (DSP) Operational Framework implementation approach

6 August 2018 (V2.1)

UNCLASSIFIED
EXTERNAL

Contents

What is the Digital service provider Operational Framework?

The Digital service provider (DSP) Operational Framework (the 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 Application Programming Interface (API) services made available through our digital wholesale channels.

The Framework is part of the ATO response in recognising and responding to the risks associated with DSPs consuming our APIs and defines a minimum set of security standards which must be met prior to DSPs consuming ATO wholesale services.

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 Framework requirements and implementation approach has been developed through a consultative 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 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

Objectives of the Framework

The 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 implemented by DSPs. Some DSPs will only consume simple, low risk services, some will only produce desktop software, and others may provide cloud services which are wholly hosted in ASD certified environments.

- **Conformance with the Framework is an ongoing expectation.**

  Ongoing participation in the ecosystem is dependent on DSPs continuing to meet the Framework requirements with annual and ad-hoc reviews conducted to ensure continued conformance.

- **The 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 necessitate continued growth and evolution to adapt and combat emerging risks or take advantage of new opportunities.

- **The 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.

Who is covered by the Framework

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

Provision of a software product or service, includes:

- commercial software
- non-commercial (freeware) or
- in house developed products.*

Note: Products or services that provide supplementary services that are not tax or superannuation related (e.g. most third 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:

Type of product/service	Applicability of scope
Desktop accounting product sold commercially	**IN scope –** DSP must complete the DSP Operational Framework Security Questionnaire
Freeware payroll product	**IN scope** – DSP must complete the DSP Operational Framework Security Questionnaire

Type of product/service	Applicability of scope
Sending service provider	**IN scope** – DSP must complete the DSP Operational Framework Security Questionnaire
Cloud based accounting platform	**IN scope** – DSP must complete the DSP Operational Framework Security Questionnaire
Payroll bureau using in house developed software	**IN scope** – DSP must complete the DSP Operational Framework Security Questionnaire
Payroll system developed in-house by an entity for the purpose of managing their own affairs, and interacting with more than 10,000 unique taxation and superannuation records	**IN scope*** – DSP must complete the DSP Operational Framework Security Questionnaire
Payroll system developed in-house by an entity for the purpose of managing their own affairs, and interacting with less than 10,000 unique taxation and superannuation records	**NOT IN scope*** – DSP is not required to complete the DSP Operational Framework Security Questionnaire
Document management system that plugs into accounting platform	**NOT IN scope** – DSP is not required to complete the DSP Operational Framework Security Questionnaire

*Note: requirements for in-house developers are currently being drafted and consulted on. It is recommended DSPs contact the Digital Partnership Office (DPO@ato.gov.au) to discuss how these requirements may apply.

In-house developers

Where a business is developing a solution to manage their own affairs, the product or service may require a unique product ID to connect to the ATO. To ATO will work with in-house developers to understand their circumstances and specific requirements they may or may not need to meet under the Framework.

To determine the applicable requirements for an in-house developer, a DSP will be required to answer the following:

- Are you developing to manage your own in-house affairs?
- Will your software be made available to any other individuals or entities?
- Is your product connecting directly to the ATO or via a data intermediary (e.g. SSP, gateway etc.)?
- Is your product desktop or cloud based?
- Is your software interacting with greater than 10,000 unique taxation or superannuation records?

Gateways or Sending service providers

A gateway, or sending service provider (SSP), is a data intermediary that facilitates the transfer of compliant electronic data messages.

DSPs operating as a data intermediary as either a Gateway or an SSP, need to respond to the additional questions with their Framework Security Questionnaire submission.

Future of the Framework

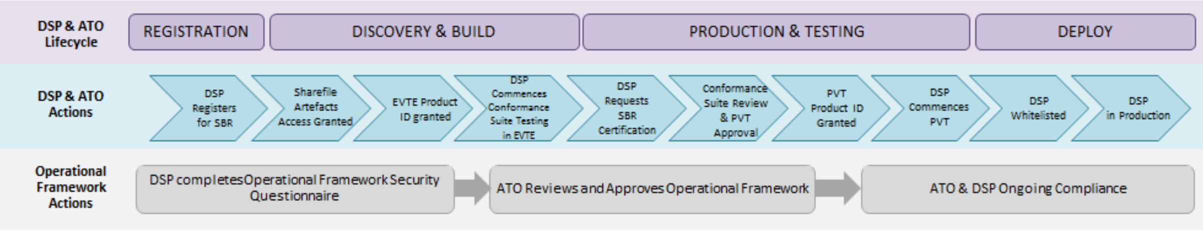
Further consultation will occur to determine a position on how the requirements apply to:

- resellers and partners
- Federal Government Agencies
- rest services/bulk data exchange
- e-Invoicing

Where the Framework fits with the DSP development process

A DSP can progress meeting the requirements of the Framework through the various stages of the development process, this includes during the design, build and test phase.

The below diagram illustrates a high level overview of the key stages for a DSP.



DSP & ATO Lifecycle
REGISTRATION
DISCOVERY & BUILD
PRODUCTION & TESTING
DEPLOY
DSP & ATO Actions
DSP Registers for SBR
Sharefile Artefacts Access Granted
EVTE Product ID granted
DSP Commences Conformance Suite Testing in EVTE
DSP Requests SBR Certification
Conformance Suite Review & PVT Approval
PVT Product ID Granted
DSP Commences PVT
DSP Whitelisted
DSP in Production
Operational Framework Actions
DSP completes Operational Framework Security Questionnaire
ATO Reviews and Approves Operational Framework
ATO & DSP Ongoing Compliance

What are the Requirements

The Framework is a scalable risk model which determines the minimum requirements a DSP must meet before consuming ATO wholesale services. Factors include:

- the API risk rating
- volume of accessible individual taxpayer or superannuation records
- the DSP's operating model

If a DSP is within scope of the Framework, a Security Questionnaire will need to be completed. Sufficient evidence will need to be supplied to support the responses provided in the Security Questionnaire.

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 Australian Government Information Security Manual (ISM) 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 ISM guidelines (see pg. 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.	
Self-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 (MFA)	(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
Sending service provider (SSP)	Not applicable

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 SSPs.

Requirements	**Low volumes of taxpayer or superannuation records (<10k)**		**Highly leveraged or high volumes of taxpayer or superannuation records (>10k)**
	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 ISM approved cryptographic algorithms and protocols (for example, TLS 1.2)		
Encryption at Rest	(Mandatory) Encryption at rest is mandatory using ISM 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 ISM guidelines (see pg. 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	(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.		
Authentication (MFA)	(Mandatory) Multifactor authentication		
Security Monitoring Practices	Not applicable	(Mandatory) Security monitoring is in place. For example: • Network / infrastructure layer • Application layer • Transaction (data) layer	
Sending service provider (SSP)	(Mandatory for SSP only) SSPs need to provide the following information: • Types of client • Service model offering • How clients connect (e.g. portal, direct API etc.)		

Note: 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

Timeframes and 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 Framework.

All new DSPs will need to seek approval under the Framework before consuming ATO wholesale services.

Existing DSPs consuming **Practitioner Lodgement Service (PLS)**, **Single Touch Payroll (STP)** or **Business Registration (BR)** services should already have approval, or be in the process of seeking approval.

Existing DSPs consuming **Superannuation** related services should be engaging with the Digital Partnership Office to understand how the requirements apply to them and when they need to be implemented. The DPO is aware of the significant investment the Superannuation industry has made already in delivering these services, and we do not want to disrupt the critical delivery of the MAAS and MATS services.

The DPO is currently engaging with a variety of stakeholders across the Superannuation industry including gateways, Gateway Network Governance Body, ASP / ASFA, fund administrators, funds and APRA to tailor a transition plan. Throughout the consultation process, updates will be provided on the software developers page so DSPs can stay informed of the progress. The ATO will also provide written confirmation of expectations and timeframes. The ATO expects DSPs to meet the requirements inline with the transition plan and will not be in breach of the requirements within the transition phase.

This transition plan will allow existing Superannuation DSPs to build and consume Member Account Attributes Service (MAAS) and Member Account Transaction Service (MATS) as they work towards meeting the requirements of the Framework.

What happens if a DSP can’t meet the transition timeframes?

The ATO recognises that each DSP is different and the suite of products and services offered can be complex. Where a DSP is unable to meet the timeframes above the ATO must be informed as soon as possible. The ATO will work with DSPs on an individual basis to develop a tailored transition approach that is mutually acceptable, taking into consideration individual circumstances. This may include the implementation of alternate controls that achieve the intended outcomes as a short term measure. The ATO is committed to ensuring consistency of appropriate security standards across the ecosystem. Where a DSP is unable to meet an agreeable transition plan, the ATO will de-whitelist an existing product.

Operational Framework approval process

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

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

- grant approval
- grant conditional approval.

Conditional Approval

Conditional approval is granted only in situations where the DSP is undertaking necessary steps to meet the Framework requirements of MFA and independent security certifications. 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.

Terms and Conditions

Each approval will include terms and conditions. Every DSP is required to accept outlined terms and conditions unique to their circumstances prior to being whitelisted.

Changing circumstances, annual, and ad-hoc reviews

The ATO will conduct an annual review of all DSPs who have been approved under the Framework. During this process, DSPs will be required to revisit the Framework requirements and provide assurance of their compliance.

The annual reassessment process ensures a DSP maintains compliance to the Framework requirements. Where certification is a requirement, evidence of currency will need to be provided. It is not expected that recertification will occur annually if the certification has, for example, a 3 year currency.

The ATO must be notified via the DPO mailbox DPO@ato.gov.au or your Account Manager (if applicable) 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
- 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 will need to provided and include updated evidence.

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

Monitoring and data breaches

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, the ATO will work with the DSP to address and limit the damage of the threat. This may include increasing the requirements a DSP needs to meet or introducing additional requirements.

The ATO will generally contact a DSP before taking action unless exceptional circumstances apply. A data or identity security breach may include:

- Identity details being accessed or seen by an unauthorised third party
- Identity details being lost or stolen due to illegal access by a third party activity (e.g. common online threats such as malware, spyware or ransomware).
- Mistakenly providing information to the wrong person, for example sending details out to the wrong email address.

Where a DSP identifies a breach through their own monitoring controls or informed directly by a client, the ATO must be notified immediately. This can be done via the DPO mailbox DPO@ato.gov.au or Account Manager (if applicable), to ensure appropriate action can be taken.

In order for the ATO to take action to limit the damage and identify the source of the threat, the following information is requested:

- appropriate contact person (specialist IT security/fraud representative)
- nature of the incident
- number of affected records
- date and timestamp
- session ID reference
- host Services (Internet Service Provider)/IP address
- device ID (ESID) if available
- TFN information
- non-TFN information (name/address/biographical information)
- product name and type (desktop or cloud)
- what format the data was in (e.g. CSV or encrypted)

Notifiable Data Breaches
In addition to the requirements of the Framework, DSPs need to be aware of The Notifiable Data Breaches scheme under Part IIIC of the *Privacy Act 1988* (Privacy Act).

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 a DSP doesn’t meet the Framework requirements?

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

What’s next

The ATO will continuously review and mature the DSP Operational Framework documentation to meet ongoing demands in technology and threats to the digital ecosystem.

- Multi-Factor Authentication (MFA)
- Superannuation
- Supply Chain technical information
- Payload Encryption technical information
- Machine to Machine (AI, bots etc.)

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

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.
ATO wholesale services	Standard Business Reporting, Rest
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).
Commercial software	Software which is produced for the purpose of on-selling.
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 breach	A data breach is an unauthorised access or disclosure of personal information, or loss of personal information. Data breaches may be caused by malicious action, human error or a failure in information handling systems.
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

Term	Definition
	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 eBMS3 standard with the addition of the AS4 profile.
Encryption	The process of encoding information in such a way that only the person (or computer) with the 'key' can decode it.
Freeware	Non-commercial software which is free to use by anyone.
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 SSP.
Hybrid model	An operating model which uses a combination of software types and connections.
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 SSP 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.
In-house developed product	A product which has been developed for exclusive use by the organisation to manage their own payroll and other affairs; the product cannot be sold to other organisations.

Term	Definition
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 SSP.
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 (SSP)	A gateway, or SSP, is a DSP that facilitates the transfer of compliant electronic data messages.
Service Organization Control 2 (SOC2)	An audit report which covers operational control systems following. 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 19 December 2017 Final Issued 8 February 2018 Update Issued 1 August 2018
Document Name	Digital service provider Operational Framework implementation approach
Document Creators	Operational Framework Lead and DPO Team
Distribution	DSP External Community ATO Internal Community
File Location	Software Developers Website https://softwaredevelopers.ato.gov.au/

Version History

Version	Changes	Date Released
0.1	Document creation and draft released	December 2017
1.0	Finalised Version Released	8 February 2018
2.0	Updated Version Released. Key changes include: • Scope of the framework as it applies to an in house developer • Updated transition strategy • Extended the requirements for sending service providers • Further clarity of annual review process and data breach processes • Removed the instructional material • How it fits into development process	2 August 2018
2.1	Updated Transition Strategy for Superannuation DSPs	6 August 2018

ato.gov.au