Australian Government
Australian Taxation Office

Digital Service Provider

Operational Security Framework Requirements

For ATO Digital Services

April 2023. V6.05

Contents

Purpose

The Digital Service Provider (DSP) Operational Security Framework (OSF) seeks to protect Taxation, Accounting, Payroll, Business Registry and Superannuation related data and the integrity of the Taxation, Business Registry and Superannuation systems that support the Australian community. This is achieved by setting out a minimum level of security requirements a DSP needs to meet in order to access ATO Digital Services that perform a functional role in the supply chain. The DSP OSF has been established to respond to business risks and security threats presented by the continual expansion and growth of digital services across the ecosystem.

The DSP OSF is a response to known examples of:

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

Scope

The DSP OSF applies to any software product or digital service that performs a functional role in the supply chain of transmitting Taxation, Accounting, Payroll, Business Registry or Superannuation data through ATO digital services.

This includes software products that **reads, stores, modifies, or routes** any Taxation, Accounting, Payroll, Business Registry or Superannuation data that:

- Connects directly to the ATO digital services
- Connects indirectly to the ATO via a sending Service Provider (SSP) for Payroll services
- Connects indirectly to the ATO via a Gateway for Superannuation Services or SuperStream.

This also includes:

- Significant modification of commercial software or white labelled products
- Non-Commercial products / In-house developers
- Products or services producing a .CSV file.

For large organisations or groups of companies, the DSP OSF may only apply to relevant systems and/or business sectors of the organisation.

Note: The scope of the DSP OSF is not intended to capture the end user who owns the data and does not perform a functional role in the supply chain e.g., a business using software to run their daily operations.

Application of Scope

Significant modification of commercial software

DSPs and users of software who customise key components of a commercial product may be regarded as in scope of the DSP OSF.

Consideration of scope includes:

- Whether the client would be classified as an in-house developer
- Any changes to the way the payloads are generated and to which it differs from the original.

Clients should contact the DPO to discuss their individual circumstances.

In-house developers

Where a product or service is being developed to manage a business's own affairs, this may be considered as 'in-house'. You will still be required to meet the requirements of the OSF however these will differ based on the size of your product e.g., Interacting with less than or greater than 10,000 Taxation, Accounting, Payroll, Business Registry or Superannuation records.

An in-house developer is a product or service that meets the following criteria:

- Be developed to manage business's own Taxation, Accounting, Payroll, Business Registry or Superannuation affairs
- Have no expectation of commercial gain
- Not be distributed outside the organisation
- Be controlled by the business

DSPs should contact the DPO to discuss individual circumstances.

Products or services producing a .CSV file

There are occasions where producing a .CSV file is in scope of the DSP OSF, where the service and the file are:

- Transformed and Transmitted via a Sending Service Provider (SSP)
- The product or service is made available commercially.

Sending Service Providers (SSPs)

The ATO seeks to understand the details of a sending service provider's (SSP) model and value chain. If a DSP will be acting in the capacity of an SSP a DSP will need to provide additional information.

Evidence required

- Intended business model e.g., will the service be offered to market
- Functional roles performed within the supply chain
- Services that will be offered e.g., file upload, portal, REST API etc.
- Architecture of the service, including services that are hosted on shared infrastructure

SSPs may also be required to provide:

- Published product description
- Screen shots displaying the method of connection

Meeting the Requirements

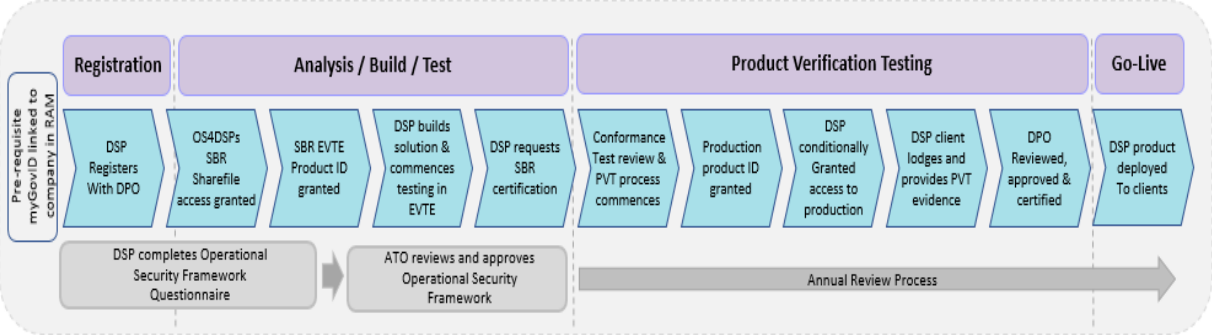
Register to access ATOs Digital Services

To access ATO APIs and Digital Services, DSPs must be registered in Online Services for DSPs (OS4DSP), a DSP will need a myGovID credential and be linked in RAM.

DSPs can commence building and testing their product in the External Vendor Testing Environment (EVTE) in parallel to undertaking the DSP OSF process including the completion of the Security Questionnaire. See the diagram below and how to start using our services for more information.

Supporting information is available in the Knowledge Hub. Additionally, DSPs can request assistance or provide feedback via OS4DSPs.

Digital Service Provider Lifecycle Overview



Determining which requirements apply to your product

The DSP OSF uses a risk scaled model to determine the relevant security controls required for your product or service. These contributing risk factors include:

- Products or services controlled by the DSP e.g., DSP cloud hosted solution
- Products and or services controlled by the client e.g., client hosted desktop solution
- Products that store or transact less than or greater than 10,000 unique Taxation, Accounting, Payroll, Business Registry or Superannuation client records
- API risk rating of the service/s consumed
- Sending Services Provider (SSP) solutions.

The DSP OSF is divided into 5 categories:

Products or services	
Category A	• Commercial product or service **controlled by DSP**, and • Low to high-risk APIs with greater than 10,000 unique client records, or • Sending Service Providers
Category B	• Commercial product or service **controlled by DSP**, and • Medium to high-risk APIs with less than 10,000 unique client records
Category C	• Commercial product or service **controlled by DSP**, and • Low risk APIs with less than 10,000 unique client records, or • No risk APIs regardless of unique client records
Category D	• Commercial product or service **controlled by client**, and • Low, medium, or high-risk APIs regardless of unique client records
	• In-House developer **controlled by client,** and • Low Risk APIs only with greater than 10,000 unique client records
Category E	• Commercial product or service **controlled by either the DSP or the client,** and • No risk APIs regardless of unique client records
	• In-House developer **controlled by client,** and • Low Risk APIs only with less than 10,000 unique client records, or • No risk APIs regardless of unique client records

Completing and submitting a questionnaire

DSPs must complete a security questionnaire and provide relevant evidence to demonstrate compliance to appropriate controls.

DSPs must submit completed questionnaires and evidence through Online Services for DSPs. DPO will contact DSPs if further information is required or will aid DSPs completing questionnaires.

DSPs with multiple products

A DSP may choose to apply the DSP OSF across their entire organisation and maintain a single accreditation for all their products and systems e.g., an independent certification may cover both products. DPO will consider one completed questionnaire when a DSP has multiple products within the same category e.g., based on their operating environment.

DSPs must clearly articulate differences between the products including any different supply chain interactions and will require supplementary evidence for any known gaps.

Note: All products must have a unique product ID.

Evidence required

DSPs must provide suitable supporting evidence to demonstrate compliance to each control requirement. Where evidence contains sensitive or confidential information a DSP may remove or redact this prior to sending to the ATO. In the event sensitive or confidential information is redacted, it must contain all relevant details to demonstrate the requirement and control has effectively been met.

Product ID

ATO provides DSPs a unique product ID for accessing both the testing and production environments. DSPs must keep the Product ID confidential and secure to ensure it is used for its intended purpose only.

- The External Vendor Testing (EVT) Product ID should only be used to access ATO testing environments for the purposes of developing and testing your product
- The production Product ID should only be used for transmission of data securely between the ATO and the product, including transmission of data through third parties.

Terms and Conditions

DSPs must accept the terms and conditions before being whitelisted to access ATO APIs in production.

- You must provide ATO with true and correct information. If you provide false or misleading information to ATO, it will result in restriction of access to services or de-whitelisting. ATO will endeavour to work through any non-compliance issues with DSPs prior to any action being taken
- Privacy and security of your personal information is important to us and is protected by law. We need to collect information and evidence so we can process and manage your application to access ATO digital services. We will not share your information with other parties, only if law allows or requires
- You are responsible for making sure your details are correct and up to date.

Conditional approval may be granted for a limited time where a DSP is undertaking independent certification. In this instance DSPs will need to provide an appropriate timeline and progress updates to the DPO and must have completed a recent self-assessment.

Letter of Confirmation

The DPO will issue all DSPs with a letter to confirm compliance with the DSP OSF controls and requirements.

Product Register

All commercial products will be listed on the ATO Product-register to provide transparency to our mutual clients. DSPs can provide the DPO with additional information to support their product register listing and should submit a ticket through OS4DSPs

Maintaining Compliance

Annual reviews

All DSPs must provide annual assurance that products remain compliant with controls and requirements of the DSP OSF. This can be completed by using the annual review ticket in OS4DSPs where DSPs are required to respond to appropriate questions with relevant evidence.

The annual review process includes a review of a DSPs self-assessment or independent certification currency. Self-assessment is deemed current for 2 years from the date of initial approval by ATO. The currency of independent certification is determined by the expiry date listed on the certificate.

If a DSP doesn't meet the requirements

The ATO expects all DSPs to meet and maintain compliance with the DSP OSF requirements. ATO is committed to the protection of Taxation, Accounting, Payroll, Business Registry or Superannuation information and will treat issues of non-compliance seriously.

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

The process outlines how de-whitelisting may occur, DSPs will not be de-whitelisted without prior notice unless extreme circumstances apply, in which de-whitelisting would be temporary.

Changes to your operating environment

DPO must be notified as soon as practicable of significant changes to the business or product environment via OS4DSPs

This may include a change to:

- Legal entity: mergers, acquisitions, divesting or large corporate restructures
- Infrastructure: new platform, hosting provider or control of the hosting environment (DSP v Client)
- Increased client base: greater than 10,000 unique Taxation, Accounting Payroll or Superannuation client records.

DPO will partner with DSPs during any changes to minimise impacts to clients. If DSPs are unsure on significance of changes, they can contact DPO via OS4DSPs

DPO reserves the right to undertake ad-hoc reviews to ensure DSPs maintain compliance to the requirements of the DSP OSF.

Data Breach

Reporting Data Breaches

A data breach occurs when personally identifiable information (PII) an entity holds is subject to unauthorised access or disclosure to an unknown party. This may be caused by a failure in security systems, information handling, human error, or malicious action. Data breaches may be identified through security monitoring practices by the DSP or the ATO.

If anomalies or areas of concern are identified by the ATO, we will work with DSPs to address and limit the damage. In these situations, ATO will contact a DSP before taking serious action e.g., de-whitelisting, unless exceptional circumstances apply.

Where a DSP identifies anomalies, breaches, or security incidents it is a requirement for DSPs to report to DPO for the ATO to mitigate damage.

A data breach may include:

- Identity details being accessed or viewed by an unknown third party
- Identity details compromised due to illegal access by third-party activity e.g., common online threats such as malware, spyware, or ransomware
- Potentially fraudulent lodgment or action resulting from compromised identity

- Mistakenly providing information to an unknown third party e.g., sending details to the wrong email address
- A breach of a third-party product or service integrating with DSP APIs.

When to report a Data Breach

A data breach should be reported to DPO immediately from the time a DSP is aware that PII data has been breached, the sooner the information is provided, the quicker ATO can implement preventative action.

After the initial reporting of the data breach, DSPs can then provide information in stages whilst undertaking their own internal investigations.

Note: Immediately is as soon as practicable and should be within a few hours.

How to Report an Incident

DSPs must report data breaches via the incident report form within Online Services for DSPs and/or via the SBR service desk on 1300 488 231. This ensures ATO can assess the risk/threat and undertake preventative action to reduce impacts to ATO or clients, including protecting any potentially compromised accounts from fraud.

For ATO to act and limit the harm caused by a data breach, the following information is required (when known):

- Appropriate contact person (specialist IT security/fraud representative)
- Nature of the breach
- 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 is in (e.g., CSV or encrypted).

Actions ATO will take post breach notification

ATO will take action to protect the integrity and confidentiality of Taxation and Superannuation systems. ATO will collaborate with DSPs where action required relates to a DSPs product. Disclosure of action taken on client records will not be provided to DSPs (due to Privacy Legislation).

Where a breach has been reported or identified ATO may take the following actions:

- Apply security measures to protect client accounts
- Provide communication direct to a user of an impacted product
- Switching off an impacted product or API
- Suspend or delay access to APIs.

Security tips for clients

- The Australian Taxation Office has security advice for tax professionals, businesses and individuals
- The Australian Cyber Security Centre has targeted guidance for individuals and business to stay safe online, including implementing the essential 8

Awareness of other obligations

In addition to the requirements of the DSP OSF, DSPs need to be aware of their obligations under:

- Notifiable Data Breach scheme under Part IIIC of the Privacy Act 1988 (Privacy Act). For further information on Notifiable Data Breach scheme, please refer to https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme
- Australian Privacy Principles, contained in schedule 1 of the Privacy Act 1988 (Privacy Act). For further information on the Australian Privacy Principles, please refer to https://www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles

Questions and Supporting Guidance

Further information regarding DSP OSF can be found within Online Services for DSPs knowledge hub. If DSPs have questions in relation to this document or completing the requirements, please contact the DPO for support.

Evolution of the Operational Security Framework

The requirements of the DSP OSF will evolve to respond to new and emerging risks. Proposed updates will be undertaken in consultation with industry representatives to establish the scale of change and appropriate transition timeframes.

Requirements for products / services

In order to identify which requirements, apply to your product or service, DSPs must first determine if the product is controlled by the DSP or the Client.

Products controlled by DSPs include:

- Cloud based environments
- Software as a Services (SaaS)
- Sending Service Providers (SSP)
- Gateways.

Products controlled by a client include:

- Desktop or local server e.g., software products hosted on the client's premise
- Cloud or Infrastructure as a Service (IaaS) controlled by the client e.g. outside the client's premise, including a single or multi-tenant infrastructure where the client has sole control of the application and control and ownership of the data
- Other scenarios may fall under 'products and services controlled by the client' beyond what is listed above.

Note: Where a DSP provides a hosted single or multi-tenanted environment for the client, access as a DSP should be limited to maintenance and support activities with client consent. DSPs in this situation must ensure each instance of the software service is unique for each client and software instances are secured through certificate exchange or Multi-Factor Authentication (MFA).

Products controlled by DSPs

Services include Cloud and Software as a Service (SaaS), Gateways and Sending Service Providers.

Requirements	Category A	Category B	Category C
	• Commercial product or service controlled by DSP, and • Low to high risk APIs with greater than 10,000 unique client records, or • Sending Service Providers	• Commercial product or service controlled by DSP, and • Medium to high risk APIs with less than 10,000 unique client records	• Commercial product or service controlled by DSP, and • Low risk APIs with less than 10,000 unique client records, or • No risk APIs regardless of unique client records
Audit Logging	**Mandatory**: Audit Logging functionality must be implemented in software products to enable traceability of user access and actions. Audit logs must be kept for a minimum 12 months.		
Authentication	**Mandatory**: Multi-Factor Authentication (MFA) must be implemented for end users and any staff member with access to Taxation, Accounting, Payroll, Business Registry or Superannuation related information of other entities or individuals e.g. Tax Agents, Employers as per Australian Government - Guidelines for system hardening • Shared logins are not permitted and must be blocked by the DSP • Remember me functionality must be limited to 24 hours • MFA should not include social media logins e.g., Google/Microsoft/Facebook. If social media applications are included in the proposed business model, DSPs should discuss with DPO.		
Certification	**Mandatory:** Independent Certification against either: • iRAP (ISM) • ISO/IEC 27001	**Mandatory**: Independent certification or Self-Assessment against either: • ISM • ISO / IEC 27001 • ISO / IEC 27002 • ISO / IEC 27017 • NIST (DPO may request evidence of some self-assessed controls)	**Mandatory**: Independent certification or Self-Assessment against either: • ISM • ISO / IEC 27001 • ISO / IEC 27002 • ISO / IEC 27017 • SOC2 • OWASP ASVS 3.0 or later • NIST
Data Hosting	**Mandatory:** Data Hosting must be onshore by default, offshore hosting arrangements, including redundant systems are managed by exception only.		
Encryption Key Management	**Mandatory:** Encryption Key Management and public key infrastructure (PKI) policy must include asymmetric/public key algorithms, hashing algorithms and symmetric algorithms as per Australian Government - Guidelines for using cryptography		
Encryption at Rest	**Mandatory:** DSPs must apply encryption at the disk, container, application or database level. Encryption at rest should follow Australian Government - Guidelines for using cryptography		
Encryption in Transit	**Mandatory:** Encryption in transit must use endorsed approved cryptographic protocol. e.g., TLS 1.2 or TLS 1.3 as per Australian Government - Guidelines for using cryptography		
Entity Validation	**Mandatory:** DSPs must implement entity validation to ensure consumers/users of a commercial software product is a legitimate business and has a genuine need to access ATO APIs.		
Personnel Security	**Mandatory:** Personnel Security procedures must be in place for hiring, managing and terminating employees including contractors.		
Security Monitoring	**Mandatory**: Security Monitoring practices must be implemented at the network/infrastructure, application and transaction layer to enable DSPs to scan environmental threats and act.		
Supply Chain	**Mandatory:** DSPs must provide ATO with an overview of their supply chain.		
Third Party Add-On	**Mandatory:** If DSPs integrate with third party add-ons via an API, they must take reasonable care to ensure appropriate security controls in place for any add-on partners. ATO recommends using the Security Standards for add-on marketplaces or an equivalent set of controls.		

Products controlled by a client

Services include Desktop and Server-based software, including Cloud applications where the application is primarily under the control of the client.

Requirements	Category D
	• Commercial product or service controlled by client and • Access to low, medium, or high-risk APIs regardless of unique client records, OR * ATO recognise DSPs may have some level of control of the requirement, the mandatory element applies where a DSP has control to implement a solution. Some controls may not be applicable.
	• In-House developer controlled by the client and • Low Risk APIs only with greater than 10,000 unique client records.
Audit Logging	**Mandatory**: Audit Logging functionality must be implemented in software products to enable traceability of user access and actions. Audit logs must be kept for a minimum 12 months.
Authentication	**Mandatory:** At a minimum, all solutions must have user-based access, including unique client logins with authentication and authorisation controls implemented e.g., unique username and password. • Shared logins are not permitted and must be blocked by the DSP • Remember me functionality must be limited to 24 hours. To strengthen your authentication, ATO recommends implementing multi-factor authentication (MFA) as best practice this can be applied as per Australian Government - Guidelines for system hardening • MFA should not include social media logins e.g. Google/Microsoft/Facebook. If social media applications are included in the proposed business model, DSPs should discuss with DPO.
Certification	**Mandatory:** Self-Assessment against either: • ISM • ISO / IEC 27001 • ISO / IEC 27002 • ISO / IEC 27017 • SOC2 • OWASP ASVS 3.0 or later • NIST
Data Hosting	**Mandatory*:** If the product provides any element of data hosting it must be onshore by default, offshore hosting arrangements, including redundant systems are managed by exception only.
Encryption Key Management	**Mandatory*:** If the product manages Encryption Key Management and public key infrastructure (PKI) policy must include asymmetric/public key algorithms, hashing algorithms and symmetric algorithms as per Australian Government - Guidelines for using cryptography
Encryption at Rest	**Mandatory*:** DSPs should apply encryption at the disk, container, application or database level. Encryption at rest should follow Australian Government - Guidelines for using cryptography
Encryption in Transit	**Mandatory:** Encryption in transit must use endorsed approved cryptographic protocol. e.g., TLS 1.2 or TLS 1.3 as per Australian Government - Guidelines for using cryptography
Entity Validation	**Mandatory:** DSPs must implement entity validation to ensure consumers/users of a commercial software product is a legitimate business and has a genuine need to access ATO APIs.
Personnel Security	**Mandatory:** Personnel Security procedures must be in place for hiring, managing and terminating employees including contractors.
Security Monitoring	**Mandatory*:** If the product has the ability to relay data to the DSP, **s**ecurity monitoring must be implemented to enable DSPs to scan environmental threats and take action.
Supply Chain	**Mandatory:** DSPs must provide ATO with an overview of their supply chain and third-party add-ons.
Third Party Add-On	**Mandatory*:** If DSPs integrate with third party add-ons via an API, they must take reasonable care to ensure appropriate security controls in place for any add-on partners. ATO recommends using the Security Standards for add-on marketplaces or an equivalent set of controls.

Commercial Products / In House Developers

Services include desktop and server-based software, where the application is under the control of the client. Category E are **primarily STP In-House developers**.

Requirements	Category E
	• Commercial product or service controlled by the DSP or the client, and • No risk APIs regardless of unique client records * ATO recognise DSPs (including in-house developers) may have some level of control of the requirement, the mandatory element applies where a DSP has control to implement a solution. Some controls may not be applicable
	• In-House developer controlled by the client and • Low Risk APIs only with less than 10,000 unique client records, or • No risk APIs regardless of unique client records
Authentication	**Mandatory:** At a minimum, all solutions must have user-based access, including unique client logins with authentication and authorisation controls implemented e.g., unique username and password. • Shared logins are not permitted and must be blocked by the DSP. • Remember me functionality must be limited to 24 hours. To strengthen your authentication, ATO recommends implementing multi-factor authentication (MFA) as best practice this can be applied as per Australian Government - Guidelines for system hardening • MFA should not include social media logins e.g., Google/Microsoft/Facebook. If social media applications are included in the proposed business model, DSPs should discuss with DPO.
Data Hosting	**Mandatory*:** If the product provides any element of data hosting it must be onshore by default, offshore hosting arrangements, including redundant systems are managed by exception only.
Encryption Key Management	**Mandatory*:** If the product manages Encryption Key Management and public key infrastructure (PKI) policy must include asymmetric/public key algorithms, hashing algorithms and symmetric algorithms as per Australian Government - Guidelines for using cryptography
Encryption at Rest	**Mandatory*:** DSPs should apply encryption at the disk, container, application or database level. Encryption at rest should follow Australian Government - Guidelines for using cryptography
Encryption in Transit	**Mandatory:** Encryption in transit must use endorsed approved cryptographic protocol. e.g., TLS 1.2 or TLS 1.3 as per Australian Government - Guidelines for using cryptography

Optional consideration for DSPs in Category E to strengthen security
• To improve the security of your ecosystem and product(s), please consider implementing the below security controls • These controls are not mandatory, and you are not required to provide any evidence of implementation • For further information regarding the below requirements, see page 15 onwards.
• Audit Logging • Certification • Multi-Factor Authentication • Personnel Security • Security Monitoring Practices

Further guidance for requirements

This section will provide DSPs with further information on each of the security control requirements, additional information is also available through Online Services for DSPs Knowledge hub.

Audit logging

Audit logging seeks to ensure traceability of access and actions within software which can be used for detection of anomalies or to support the investigation of a security incident. In the event of a security incident, relevant audit logs will need to be supplied to the ATO.

Audit logging needs to include:

- Access and event-based logs including changes to privileges, permissions and authorisations.
- Users with privileged access must also be identifiable within these logs
- Shared login credentials are not permitted, and each individual user and session will need to be uniquely identifiable through audit logs
- Logs must be kept for a minimum of 12 months and must not be deleted within this period.

Evidence required

DSPs must provide dummy or authentic access and event logs (sensitive information redacted) which include:

- Authentication and authorisation
- Date and time of the event
- Username / identifier
- Success or failure of the event
- Event description
- ICT equipment location and identification

DSPs can provide an audit log policy to cover the inclusions requested (retention, no shared logins etc).

It is recommended DSPs adopt a risk-based approach to implement controls from the Australian Cyber Security Centre Guidelines-System-Monitoring or equivalent industry standard such as NIST Guide to Computer Security Log Management

Authentication

Multi-Factor Authentication (MFA)

Multi-factor authentication (MFA) is defined as a method of authentication that uses two or more authentication factors from different categories, to authenticate a single claimant to a single authentication verifier.

The authentication factors can be categorised as:

- Something you know, such as a password or a response to a security question
- Something you have, such as a one-time pin, SMS message, smartcard, or software certificate
- Something you are, such as biometric data, like a fingerprint or facial geometry.

Single-factor authentication generally falls into the 'something you know' category such as a password. MFA requires a user to prove they have physical access to a second factor that they either have (e.g., a physical token) or are (e.g., fingerprint).

MFA for DSP controlled environments

This requirement seeks to minimise the opportunity for unauthorised users to access Taxation, Accounting, Payroll, Business Registry or Superannuation related information.

- All cloud environments must have MFA in place to access any data in scope of the DSP OSF
- MFA is required for all users of software products that are controlled or hosted by the DSP
- MFA is required for all DSP staff with privileged user access
- Inactive Session time-out occurs after a maximum 30 minutes (15 minutes is preferred). This is a screen lock process where full MFA is not required to unlock.
- Remember me on this device to be limited to 24 hours
- Tokens or temporary credentials should be isolated to an individual device and expire once used. Any token or temporary credential must expire within 24 hours
- Brute force lockouts are applied after a maximum of 5 unsuccessful login attempts. This specifies that an event must occur, not how each DSP handles this lockout before a client can re-try logon. We do not seek the details of the lockout process, only that it occurs.
- Shared logins are not permitted and need to be blocked by the DSP. Each individual user and session will need to be uniquely identifiable through audit logs
- Authenticator apps can be used e.g., Microsoft Authenticator, Symantec VIP or Google Authenticator and will need to demonstrate how MFA is enforced at login
- Social media credentials are not recommended to be used for MFA e.g., Google/Microsoft/Facebook to sign in, however if your solution is based on the use of social media credentials you must contact the DPO to discuss your proposed solution
- Use of enterprise SSO logins require technical assessment and approval by the ATO.

Further information on each method can be found at ACSC: Implementing Multi Factor Authentication.

DSPs that have not implemented MFA, should consider implementing passphrase management, account lockout and resetting passphrase practices described in the Australian Government - Guidelines for system hardening

Single Sign On

DSPs must seek advice from the DPO on the use of enterprise SSO to support their clients.

In implementing Enterprise SSO DSPs must ensure that:

- Disablement of MFA is controlled by the DSP, not the client
- Encryption in transit between the client's system and software uses as an approved protocol as per the Australian Government - Guidelines for using cryptography.
- Remember me on this device to be limited to 24 hours
- SSO tokens must be limited to a maximum period of 24 hours
- Tokens or temporary credentials should be isolated to an individual device and expire once used. Any token or temporary credential must expire within 24 hours
- SSO occurs behind the client's enterprise firewall e.g., gateway
- Brute force lockouts are applied after a maximum of 5 unsuccessful login attempts
- Credentials are stored separately from the system which grants access
- Confirmation passwords are hashed, salted, and stretched
- Inactive Session time-out occurs after a maximum 30 minutes (15 minutes is preferred). This is a screen lock process where full MFA is not required to unlock.

- ACSC Authentication Hardening includes additional guidance to support DSPs implementation.

Note: Short Message Service (SMS), are more susceptible to compromise by an adversary than others. As such ATO recommends utilising an alternative authentication factor when appropriate.

Evidence required

Provide **all** the following details:

- User description paired with screen shots of MFA workflow that cover the process Login, Challenge, Success, and Failure.

- Password or access control policy which demonstrates:

    - user access controls
    - remember me functionality
    - idle session time-out
    - brute force lockouts
    - token or temporary credential expiration
    - confirmation in writing that no social media log in used

Note: DSPs may also be required to provide a live or mock demonstration of the MFA process to support their evidence provided.

Certification

Independent Certification

The independent certification requirement seeks to provide the ATO with a level of assurance a DSP has robust security practices in place across the organisation.

This is done by way of attaining independent certification against one of the below standards:

- iRAP
- ISO/IEC 27001

As part of the independent certification exercise, a DSP will need to determine which controls from the chosen standard apply to your organisation. Where a DSP deems a control not applicable this should be addressed in the statement of applicability.

The ATO are unable to prescribe which of the above methods a DSP should apply or provide links to them. The choice of what standard to complete independent certification against should be made based on its suitability to your organisation.

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

DPO recognises a DSP may not be fully compliant with the complete range of controls of their chosen standard. The controls a DSP should be compliant with will be dependent on the organisation's operating model and the architecture of the product. We also acknowledge there may be areas where a DSP is unable to demonstrate compliance with controls. In these scenarios a DSP will be required to offer supporting commentary to substantiate the non-compliance or the manner / timeframe in which a DSP is expected to address the gap.

Independent certification should be reviewed at prescribed intervals or when significant changes occur within the environment. To meeting the requirement for independent certification, a DSP must maintain ongoing independent certification. This evidence needs to be supplied to the ATO. Where a DSP has a significant change in the environment which affects the controls you have addressed as part of independent certification, DSPs are required to submit a revised version to the ATO as soon as possible.

IRAP / ISM

The ASD's Information Security Registered Assessors Program (iRAP) accredits ICT professionals to assess organisations against the Australian Government's Information Security Manual (ISM). An iRAP assessment will typically cover the organisation as a whole, (governed by a defined scope), and it assesses 24 key security domains against the ISM. iRAP assessments may be mandated as a firm requirement, for commercial entities seeking to offer ICT services to federal government agencies as part of formal procurement / tendering processes.

ISO/IEC 27001

ISO 27001 is generally completed at the organisational level, however large organisations with diverse service/product offerings may limit the scope of the independent certification to relevant policies, procedures, and systems of the business unit responsible for the primary products or services which hold or transact Taxation, Accounting, Payroll, Business Registry or Superannuation data.

To obtain independent certification, a DSP is required to engage a qualified, independent assessor annually to conduct an audit of their business in relation to the standard.

Evidence required

Provide one of the following:

- copy of certificate
- letter of compliance and final report

If seeking conditional approval for independent certification:

- letter of engagement with a start date, completion date, scope of work and assessor details needs to be provided.

Self-Assessment

The self-assessment requirement seeks to provide ATO with a level of assurance a DSP will have robust security practices in place across the organisation. This is done self-assessing against one of the below standards:

- ISO/IEC 27001
- ISO/IEC 27002
- SOC2
- OWASP ASVS 3.0 or latest version
- NIST

As part of the self-assessment, a DSP will need to determine which controls from the chosen standard apply to the organisation. Where a DSP deems a control is not applicable a short description should be provided as to why.

The scope of certification should cover relevant organisational policies, procedures and data repositories that hold or manage Taxation, Accounting, Payroll, Business Registry or Superannuation related information.

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

DSPs can request to use an alternative security standard if a DSP determines it is more suitable for the circumstances. These requests will be assessed on a case-by-case basis.

The ATO are unable to prescribe which of the above methods a DSP should use. The choice of what standard to self-certify against should be made based on its suitability to the organisation.

The DPO recognises DSPs may not be fully compliant with the complete range of controls of the chosen standard. The controls a DSP should be compliant with will be dependent on your organisation's operating model and the architecture of the product. We also acknowledge there may be areas where a DSP is unable to demonstrate compliance with controls. In these scenarios the DSP will be required to offer supporting commentary to substantiate the non-compliance or the manner / timeframe in which the gap is expected to be addressed.

Your self-assessment should be reviewed at prescribed intervals or when significant changes occur within your environment. To meet the framework requirement for self-assessment, DSPs must review your self-assessment annually and resubmit an updated version every 2 years. Where a DSP has had a significant change in the environment which affects the controls you have addressed as part of your self-assessment, a DSP is required to submit a revised version to the ATO as soon as possible.

ISO/IEC 27001

ISO/IEC 27001 is generally completed at the organisational level, however large organisations with diverse service/product offerings may limit the scope of the self-assessment to relevant policies, procedures, and systems of the business unity response for the primary products or services which hold or transact Taxation, Accounting, Payroll, Business Registry or Superannuation data.

All controls need to be answered, with notes next to each control as to how the DSP has achieved compliance or why the control does not apply. We don't expect a DSP to be compliant with all the controls. This will be dependent on the organisation's operating model and the architecture of the product.

ISO/IEC 27002

ISO/IEC 27002 provides guidance for organisational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organisation's information security risk environment(s).

It is designed to be used by organisations intending to:

- Select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001
- Implement commonly accepted information security controls
- Develop their own information security management guidelines.

ISO/IEC 27017

ISO/IEC 27017 provides guidelines for information security controls applicable to the use of cloud services by providing an additional implementation guidance for 37 controls specified in ISO/IEC 27002 and 7 additional controls related to cloud services.

OWASP ASVS 3.0

OWASP ASVS 3.0 is completed at the product/application level.

OWASP ASVS 3.0 controls need to be completed to Standard 2 as a minimum, with notes next to each control as to what a DSP needs to do to manage the control and if a control doesn't apply to the product why it doesn't apply. We don't expect a DSP to be compliant with all Standard 2 controls, this will be dependent on the product's architecture.

SOC2

SOC2 is generally completed at the product/application level.

SOC stands for "system and organizational controls" and is a collection of control criteria related to how organisations regulate their information. Some controls include risk management, change management, system operations, logical and physical access controls and monitoring of controls. SOC2 is the most comprehensive in the SOC family and it is most suited to IT service providers.

NIST

NIST is to be completed via a maturity assessment.

The National Institute of Standards and Technology (NIST) is a policy framework of computer security guidance to assess and approve an organisations security posture to respond to prevent and detect cyber-attacks. The framework is devised into five main functions of identity, protect, detect, respond, and recover. These functions support an organisation in expressing a level of cyber security risk by addressing threats and developing learnings.

NIST can only be applied to Category B (medium to high-risk APIs) and Category C (low to no risk APIs) DSPs.

Evidence required for Self-Assessment

Completed documentation demonstrating your conformance, with comments covering all the requirements (full control suite) of one of the approved security standards.

Note: Self-Assessment needs to be renewed every 2 years, with evidence of the latest self-assessment provided during the Annual Review process.

Data hosting

DSPs must provide details of their hosting provider to the ATO. This requirement seeks to limit the risk of access to Taxation, Accounting, Payroll, Business Registry or Superannuation related information by individuals with no authority to access, including foreign actors.

By default, a DSP should host data onshore. Offshore hosting arrangements will be managed by exception on a case-by-case basis. Where a DSP is planning to host data offshore, additional evidence will be required to satisfy the data hosting requirement.

Where DSPs have a compelling reason for storing data outside of Australia a DSP must consult with the ATO to ensure impacts have been adequately addressed. As part of this consultation DSPs must demonstrate they have considered the jurisdictional constraints.

ATO's preference is for all redundancy locations to mirror the primary production environment. Where strong encryption controls and alignment to APRA Prudential Practice Guide CPG 235 Managing Data Risk and APRA Prudential Practice Guide SPG 231 Outsourcing are applied you may discuss with ATO on suitability of redundancy hosting arrangements in an offshore location. Applications will be reviewed on a case-by-case basis.

Consistent with APRA Prudential Practice Guide CPG 235 Managing Data Risk, ATO expects 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.

Consistent with APRA Prudential Practice Guide SPG 231 Outsourcing, ATO expects DSPs would complete a risk assessment against the below risks which include steps to mitigate identified risks:

- **Country risk:** 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 you as the DSP.
- **Compliance (legal) risk:** risk that offshoring arrangements will have an impact upon your ability to comply with relevant Australian and foreign laws and regulations (including accounting practices)
- **Contractual risk**: risk that your ability as a DSP to enforce the offshoring agreement may be limited or completely negated
- **Access risk**: risk that your ability as 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
- **Counterparty risk**: risk arising from the counterparty's failure to meet the terms of any agreement with you as a DSP or to otherwise perform as agreed.

ATO expects that an offshoring arrangement would typically include a provision around security and confidentiality of information.

Where a DSP is storing data outside of Australia they must:

- Make it clear to 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 e.g., clients of tax practitioners, employees, etc. on where and how their data is being managed.

Evidence required

- Provider name
- Provider location (region)
- Redundancy location (region)
- Whether the provider is ASD certified or assessed against another security standard

If you are storing data offshore you will need to contact the DPO.

Encryption key management

DSPs need to demonstrate a policy or process is in place to govern the lifecycle management of encryption keys and minimise the risks of compromised keys.

The scope of this policy should cover three categories:

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

The use of algorithms must align to the Australian Government - Guidelines for using cryptography.

A key management policy/plan must include generation, distribution, storage, renewal, revocation, recovery, archiving and destruction of encryption keys. For more information see attachment F of APRA Information Security CPS 234

Evidence required

- Copy of key management policy/plan which includes:
  - Generation
  - Distribution
  - Storage
  - Access
  - Renewal
  - Revocation
  - Rotation
  - Archiving
  - Length and complexity of keys
  - Destruction of compromised encryption keys
  - Recovery

Note: Where encryption keys are managed by a third-party provider, confirm this by providing evidence to show a relationship, such as an email or contract/agreement with your provider.

Encryption at rest

The scope of encryption at rest covers data stored for the purpose of Taxation, Accounting, Payroll, Business Registry and Superannuation transactions including Personally Identifiable Information (PII).

The approved symmetric encryption algorithms are Advanced Encryption Standard (AES) using key lengths of 128, 192 and 256 bits, and Triple Data Encryption Standard (3DES) using three distinct keys as per the Guidelines for using Cryptography.

DSPs can choose to apply this control by either encrypting the disk, container, application, or database. Alternatively, DSPs may choose to apply partial encryption to data at the block, field, or column level but this must cover data that is stored for the purpose of Taxation, Accounting, Payroll, Business Registry and Superannuation transactions including Personally Identifiable Information (PII).

For DSPs who have implemented encryption at rest, further controls are recommended with information to implement network segmentation and segregation found at ACSC Implementing Network Segmentation and Segregation

Evidence required

One of the below is suitable evidence:

- Screenshot showing encryption enabled, confirmation of method of encryption applied, and algorithm used
- Licensing agreement or invoice with whitepaper
- Policies relating to data classification when applying block, field, or column level encryption

Where encryption at rest is not viable, provide a screenshot/policy which demonstrates all the below have been met

- User/system role-based access controls and active logging and monitoring protocols
- Restricting or limiting access to databases using the principle of least privilege
- Separation of hosts and segregation of networks or micro segmentation
- Intrusion Prevention and detection controls.

Further information is available at ACSC Implementing Network Segmentation and Segregation

Encryption in transit

To protect the confidentiality and integrity of Taxation, Accounting, Payroll, Business Registry and Superannuation information in transit.

DSPs need to provide evidence of an approved protocol TLS 1.2 or higher is used as per Guidelines for using Cryptography and Annex A of ACSC Implementing Certificates, TLS, and HTTPS.

Evidence required

All cloud products must provide one of the following:

- Back-end configuration of TLS (e.g., load balancer)
- SSL labs report for public certificates

All indirectly connecting products must provide one of the following:

- Licensing agreement with SSP
- Screenshots from SSP portal
- Screenshot of API call to 3rd party showing TLS protocol.

Note: Desktop products that directly connect to the ATO are not required to provide evidence for this requirement.

Entity Validation

Entity Validation ensures that the consumer/user of a commercial software product is a legitimate business and has a genuine need to access a DSPs software.

To complete entity validation a DSP must verify the entity against a reliable and independent source e.g., the Australian Business Register. Additionally, DSPs must ensure they have valid client contact details, including a confirmed email and phone number. Customers who do not have an ABN for example a student using software for research purposes are only required to validate the client contact information.

Note: Entity Validation does not negate the need for DSPs to meet specific service requirements relating to verification e.g., SuperMatch requires specific customer verification requirements as part of the terms of use.

Evidence required

Provide **all** the following:

- policy or process that demonstrates entity validation is in place as part of the product registration and/or purchase process.
- advise how you verify the ABN is active
- advise how you verify the contact number and email are valid

Personnel Security

This requirement seeks to mitigate threats from malicious internal actors (trusted insiders).

You need to demonstrate appropriate processes and procedures are in place for hiring, managing, and terminating employees and contractors. Processes and procedures may include but are not limited to:

- Identity proofing/pre-employment screening
- Previous employment checks
- Police checks
- Employee obligations
- Separation activities

Micro DSPs (up to three employees) are exempt from this requirement unless contractors or non-employees have access to source code or Taxation, Accounting, Payroll, Business Registry or Superannuation related information.

Evidence required

- Internal policy document detailing how employees maintain confidentiality of enterprise information
- Process descriptions detailing pre-employment screening and separation procedures or
- Sample contracts detailing conditions of employment.

Micro DSPs

Confirm that contractors or non-employees do not have access to the source code.

If they do Personnel Security provisions will apply.

Security monitoring

This requirement seeks to minimise the risk and impact of cyber incidents by having controls in place to detect, prevent and respond to cyber-attacks.

Monitoring is a joint responsibility between the ATO and a DSP. Where relevant DSPs must demonstrate appropriate monitoring of networks, applications and transactions are in place. DPSs must also be able to demonstrate they scan their environment for threats and will take appropriate action where anomalies are detected.

Evidence required

- Screenshot of an intrusion detection system such as a firewall that generates alerts
- Approach to detect anomalies or a screenshot of a security event and incident management dashboard
- Intrusion prevention system which protects end points and scans the DSP environment to prevent malicious events
- Policy demonstrating actions that will be taken where anomalies are detected.

Supply Chain

Supply chain visibility seeks to identify entities and their functional roles involved in the transmission of information, operating to and from the system which generates the payload and the ATO. This includes providing details of any third-party connections to your product via APIs.

The functional roles within a supply chain can be 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 and/or 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 subset or additional derived/calculated data
- **Data Transformer:** Party responsible for changing representation of data to file format of data (e.g., CSV to XML)
- **Data Provider:** Party responsible for the payload (which may be encrypted)
- **Data Transmitter:** Party responsible for the message with the payload. (e.g. ebMS3/AS4 transmission). These requirements are an interim measure only and may change when the supply chain visibility solution is available.

Evidence required

DSPs are required to provide the business details of the participants in the supply chain including:

- Entity name
- ABN
- Service provider role or function

DSPs with an add-on marketplace will need to provide additional information.

Third Party add-on marketplaces

The requirement seeks to identify security controls and policies DSPs need to implement, when partnering with third party add-on providers and allow connection via an API. For this purpose, SSPs and gateways are not considered as DSPs with add-on marketplaces.

Examples of add-ons:

- Accounting/Taxation: inventory, CRM, OCR scanning
- Payroll: timesheets, rostering, pay calculator
- Superannuation: audit integrations, share registries.

You must provide details of the security standard adopted to govern your third-party add-on providers, including evidence that your ecosystem partners have met SSAM or an equivalent.

You must provide details of all developers of third-party add-on marketplaces that connect to your product.

We define ‘Add-on marketplace’ as an:

- API that is offered by a DSP for use by other third-party software developers to provide additional value-added services to end customers.

Evidence required

Provide all the following details:

- copy of the security standard adopted to govern your third-party add-on providers
- a list of your third-party developers including names and a hyperlink to their website.

An attached spreadsheet is the preferred format for the list.

We recommend the Security Standard for Add-on Marketplaces (SSAM) as a baseline.

The Security Standard for Add-on Marketplaces (SSAM) provides guidance for cloud based third party add-ons who integrate via API with Digital Service Providers (DSPs). The standard applies to third party add-on developers with connections to Australian business customers of a DSP or those who are connected to the practice client list of an Australian tax or BAS agent (practice connection).

Acronyms

Further definitions can be found via Online Services for DSPs

Acronym	Definition
ABN	Australian Business Number
ACSC	Australian Cyber Security Centre
ASD	Australian Signals Directorate
API	Application Programming Interface
ATO	Australian Taxation Office
CSV	Comma Separated Values
DPO	Digital Partnership Office
DSP	Digital Service Provider
EVT	External Vendor Testing Environment
ISM	Information Security Manuel
MFA	Multi-Factor Authentication
OS4DSPs	Online Services for DSPs
OSF	Operational Security Framework
SSAM	Security Standards for Add-on Marketplace
SaaS	Software as a Service
SBR	Standard Business Reporting
SSO	Single Sign On
SSP	Sending Service Provider
TFN	Tax File Number

Document Details

Attributes	Details
Version	6.04
Date updated	November 2022
Document Name	Digital Service Provider, Operational Security Framework
Contact	Online Services for DSPs or DPO@ato.gov.au

Versioning

Version	Changes	Date Released
0.1	Document creation and draft released	Dec 2017
1.0	Finalised version released	Feb 2018
2.0	Major version released key changes include: • Scope of the Framework as it applies to an in-house developer • Updated transition strategy • Extended requirements for Sending Service Providers (SSP) • Clarity for annual review process and data breaches • Removed instructional material	Aug 2018

3.0	Major version released key changes include:
	• Scope and requirements updated
	  ○ In-house DSP description
	  ○ Significant customisation of commercial software
	  ○ Refined scope in context of large and/or diverse organisations
	  ○ Updated definition of client hosted to client controlled
	• Multi-factor authentication requirements and guidance
	• Alternate controls to protect data at rest, encryption at rest
	• Clarification of payroll data
	• Details of annual review and changing circumstances process
	• What happens DSPs don't meet the framework
	• Evolution of the framework
	• Intent, examples of evidence and further guidance for requirements
	• Glossary included
		Dec 2018

4.0	Updated wording to align with the DSP Operational Framework Security Questionnaire (Version 1.3).	Jun 2019
5.0	Added requirements for DSPs with add-on marketplaces.	Oct 2019

5.1	Minor updates: • Clarification on approval process and requirements for using Single Sign On (SSO) on for enterprise customers. • Link included to de-whitelisting process document.	Jan 2020
6.0	Major Update Released: • Version 6.0 • Complete document re-write with hardened security controls in response to a maturity review, see Operational Framework Review Working Group | ATO Software Developers Website.	Aug 2021
6.01	Minor Update Released: • Version 6.01 • Language correction relating to categories of Commercial Product & In-House developers within the requirements tables.	Sept 2021
6.02	Minor Update Released: • Version 6.02 • Reduction of requirements in Category E.	Sept 2021
6.03	Minor Update Released: • Version 6.03 • Update to wording to clarify Category E as In-House, MFA requirements (Inactive Session timeout and Brute Force), Data hosting (Region)	May 2022
6.04	Minor Update Released: • Version 6.04 • Update to wording to clarify data breach information • Not required to report incidents contained in DSP environment	November 2022
6.05	Minor Update Released • Version 6.05 • Updates to evidence requirements to match Questionnaire March 2023 release, including Multi Factor Authentication, Certification, Encryption Key Management, Encryption at Rest, Encryption in Transit, Entity Validation, Personnel Security, Supply Chain and Third-Party Add-On wording, removing 1000 connections.	April 2023

ato.gov.au