Australian Government
Australian Taxation Office

DRAFT FOR FEEDBACK

DSP Operational Framework

Requirements to utilise ATO digital services

Overview

Key changes

Key changes since the last update (August 2018), include:

- Guidance provided on multi-factor authentication requirements
- Refined definition of an in-house DSP
- Refined scope in the context of large and/or diverse organisations
- Updated the definition of client hosted to client controlled
- Alternate controls to protect data at rest (encryption at rest)
- Intent, examples of evidence and further guidance notes for each requirement

Intent

The Digital Service Provider (DSP) Operational Framework (the Framework) has been established to respond to the business risks and security implications presented by the growth of our digital services across the digital economy.

The Framework seeks to protect tax or superannuation related information as well as the integrity of the taxation and superannuation systems which support the Australian community. This is achieved by setting out the minimum level of requirements a DSP needs to meet in order to consume ATO services. The Framework 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

Where DSPs provide a software product or service that reads, modifies or routes any tax or superannuation related information then that product or service is in scope of the Framework and will need to meet the requirements. This includes DSPs that use an intermediary such as a gateway or sending service provider (SSP) to interact with the ATO.

Application of the scope in different circumstances

In-house developers

Where a product or service is being developed to manage a business's own affairs, it may be deemed as 'in-house' and fall outside the scope of the Framework.

Although products or services deemed as in-house do not need to meet all the requirements of the Framework, we strongly suggest its adoption as good practice.

To be considered as in-house, the product or service must meet all of the following criteria:

- Be developed to manage the business's own taxation, superannuation or payroll affairs only
- Have no expectation of commercial gain
- Not be distributed outside the organisation
- Be controlled by the business
- Interact with less than 10,000 taxation or superannuation records

Products deemed as in-house, will be provided with terms and conditions that you will be required to accept.

Significant modification of commercial software

Clients who customise commercial software products or services to an extent where it is no longer supported or maintained by the provider may be regarded as in scope of the Framework. In these circumstances, consideration will be given to:

- whether the client would be classed as an in-house developer,
- any changes to the way that the payload is generated, and
- the extent to which the payload generated by the customised solution differs from the original.

Clients should contact the ATO to discuss their individual circumstances.

DSPs providing diverse product/service offering beyond tax and super

Large organisations with diverse service/product offerings, may limit the scope of the framework to relevant policies, procedures and systems of the business unit responsible for the primary products or services which hold or transact tax or super information. This should be done in consultation with the ATO.

DSPs that are part of a group of companies

If you are part of a large group of companies, you may limit the scope of the framework to relevant policies, procedures and systems of the business unit responsible for the primary products or services which hold or transact tax or super information. This should be done in consultation with the ATO.

Products or services producing a .CSV file

Where you develop a product or service that produces a .csv or similar file which is then transformed and transmitted via an SSP, and you make that product or service available commercially, it is in scope of the Framework.

Evolution of the Framework

The requirements of the Framework will change over time to respond to new and emerging risks. Proposed updates will be consulted with industry and their representatives, before being finalised. DSPs that have been approved or working towards approval will be given reasonable time to transition to meet the updated requirements.

Requirements

Understanding how the requirements apply to you

The requirements you will need to meet in order to be approved under the Framework and start consuming ATO services is dependent on a few factors:

- the API risk rating of the service/s you are looking to consume
- whether the product or service you are developing transacts with a volume of greater than 10,000 accessible individual taxpayer or superannuation records
- your operating model (eg: product or service is controlled by the client or controlled by the DSP).

Requirements for products and services controlled by the client

Client controlled products and services include desktop software and server based software where the application is primarily under the control of the client.

Examples can include but are not limited to:

- A desktop solution hosted on the client's premise
- A server or cloud solution hosted on infrastructure or a tenant controlled by the client
- A server or cloud solution hosted by the DSP in multi-tenant infrastructure where the client has 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.

In the case of a DSP providing a hosted 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 that:

- End-points are unique for each client
- End-points are secured through certificate exchange or multi-factor authentication

Single-sign on (SSO) to a DSP hosted multi-tenanted environment is permitted.

Where the above conditions are not met see *'Requirements for products and services hosted by the DSP'*.

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 must 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.
Encryption key management	(Optional) Must be met where data is encrypted at rest. Encryption key management (including Public Key Infrastructure (PKI) keys) complies with ASD / ISM guidelines (see pg. 259-262)	
Audit logging	(Mandatory) Appropriate audit logging functionality implemented	
Product ID in message header	(Mandatory for all SBR services) The Product ID of the software that produces the payload information must be included in the message. This requirement does not apply to SuperStream messages.	
Certification	(Mandatory) Self-assessment against either: • iRAP, • ISO/IEC 27001, • OWASP ASVS3.0 or • SOC2	
Supply chain visibility	Not applicable	(Mandatory where payload encryption is not implemented) The supply chain visibility solution is being developed in the near future. Interim measures are in place.
Data hosting	Not applicable	
Multi-factor authentication	(Optional) The ATO recommends that multi-factor authentication (MFA) is applied, or the option is made available where practical to do so. DSPs that have not implemented MFA, should consider implementing passphrase management, account lockout and resetting passphrase practices described in the Information Security Manual pg 195.	
Security monitoring practices	(Mandatory) DSPs that utilise web services (e.g. hybrid desktop environments) and are consuming medium and high risk APIs are required to have security monitoring in place. For example: • network / infrastructure layer	

	• application layer • transaction (data) layer

Requirements for products and services controlled 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)**
	Consumes no/low risk APIs only	**Consumes medium or high risk APIs**	
Personnel security	(Mandatory) A personnel security integrity check process must 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 for data repositories that hold or manage tax or superannuation related information 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 where supply chain visibility is not implemented) Payload encryption solution is not currently available, but will be developed in the near future.		
Encryption key management	(Mandatory) Encryption key management (including Public Key Infrastructure (PKI) keys) complies with ISM guidelines (see p.g. 259-262).		
Audit logging	(Mandatory) Appropriate audit logging functionality implemented		

Product ID in message header	(Mandatory for all SBR services) The Product ID of the software that produces the payload information must be included in the message. This requirement does not apply to SuperStream messages.		
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 where payload encryption is not implemented) The supply chain visibility solution is being developed in the near future. Until then, interim measures are required.		
Data hosting	(Mandatory) Data hosting is onshore by default. Offshore hosting arrangements (including redundant systems) are managed by exception only.		
Authentication	**End users accessing the product or service** (Mandatory) End users that can access taxation or superannuation related information of other entities or individuals (e.g. tax agents, employers) (Optional but recommended) End users that only have access their own information and do not have access to taxation or superannuation related information of other entities or individuals. (E.g. employees accessing employee portals) **DSP Staff (including contracted labour)** (Mandatory) DSP staff with access taxation or superannuation related information. This position applies unless the DSP can adequately demonstrate that the internal user does not perform a privileged administration role (system / database level) and the full range of compensating controls specified within the Information Security Manual control material (pages 192 – 195)		

	have been suitably implemented. (Optional but recommended) DSP staff (other than privileged users) without access to taxation or superannuation related information of other entities. **Note** Tokens or temporary credential should be isolated to an individual device and expire once used. Any token or temporary credential should expire within 24 hours. DSPs that have not implemented MFA, should consider implementing passphrase management, account lockout and resetting passphrase practices described in the Information Security Manual pg 195.	
Security monitoring practices	Not applicable	(Mandatory) Security monitoring is in place. For example: • network / infrastructure layer • application layer • transaction (data) layer
Sending Service Provider	(Mandatory for Sending Service Providers only) Sending Service Providers need to provide the following information: • Types of client • Service model offering How clients connect (e.g. portal, direct API etc)	

Further guidance on the requirements

You must provide suitable supporting evidence to demonstrate that all applicable requirements of the Framework have been met. Where evidence contains sensitive or confidential information you may remove this prior to sending through to the ATO. For the evidence to be acceptable in the event sensitive or confidential information is removed, it must still contain all the relevant details to demonstrate that the requirement has been met.

Personnel security

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

You need to demonstrate that 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
- Qualification checks
- Previous employment checks
- Police checks
- Employee obligations
- Separation activities

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

Notes

Micro businesses (one or two employees) are exempt from this requirement unless contractors or non-employees have access to source code or taxation or superannuation related information. You will be required to provide written confirmation that this is the case.

Encryption in transit

This requirement seeks to protect the confidentiality and integrity of taxation or superannuation related information in transit.

You need to provide evidence that your product or service utilises TLS 1.2 or another ISM approved cryptographic algorithm and/or protocol. If you use an SSP and they are providing encryption in transit, you will need to demonstrate your relationship with the SSP.

Evidence required

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

- SSL certificates
- Showing HTTPS protocol being enforced

- Call to REST API
- TLS handshake protocol being enforced

When using an SSP/Gateway to indirectly connect to the ATO:

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

Encryption at rest

This requirement seeks to protect taxation or superannuation related information from unauthorised access.

You can chose to apply encryption at the disk, container, application or database level. Encryption at rest should follow ISM approved cryptographic algorithms and protocols.

Evidence required

Evidence could include:

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

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

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

Notes

The scope of encryption at rest covers data repositories that hold or manage tax or superannuation related information.

Payload encryption

This requirement seeks to protect the confidentiality and integrity of taxation or superannuation related information from the source to the end point.

Payload encryption is the preferred solution for transporting sensitive or classified information through a supply chain. You must, at a minimum, implement either payload encryption or supply chain visibility requirements.

Notes

Payload encryption solution is yet to be developed and as such compliance against this requirement is not mandatory at this stage.

Encryption key management

This requirement seeks to minimise the risks of compromised encryption keys.

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

Evidence required

Key Management Plan should cover the generation, distribution, storage, access, renewal, revocation, rotation, length and complexity of keys, recovery, archiving and destruction of compromised encryption keys.

Audit logging

This requirement seeks to ensure traceability of access and actions.

Audit logging should include both application level (access logs) and event based actions. Audit logs are not required to be submitted to the ATO on a regular or ongoing basis. You will need to be able to access or supply the logs on the occurrence of a security event where further investigation of the data is required.

Evidence required

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

Notes

Audit logging standards are based on a number of key components. You should consider your environment and what logging should be implemented and ensure that the logging records include following where applicable:

- Date and time of the event
- Relevant user or process
- 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))

Product ID in message header

This requirement seeks to ensure visibility of the software product or service that initiated a transaction.

Sending Service Providers must ensure that the product ID of the software that produced the payload information is included in the message header. Software products or services that export a flat file (eg csv) for transmission via an SSP must have a unique Product ID.

Evidence required

Screen shot of the product ID in the message header.

Notes

This requirement only applies to SBR services. This requirement does not apply to SuperStream services.

Certification (Self-assessment)

The certification requirement seeks to provide the ATO with a level of assurance that you have robust security practices in place across your organisation. This is done by way of self-assessing against one of the below standards:

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

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

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

The ATO are unable to prescribe which of the above methods you should use. The choice of what standard to self-assess against should be made on the basis of suitability to your organisation.

We don’t expect you to be compliant with all the controls of your chosen standard. The controls that you should be compliant with will be dependent on your organisation’s operating model and the architecture of your product. We also acknowledge there may be areas where you don’t fully meet a control but have indicated that you will work to address the gap over time.

Your self-assessment should be reviewed at prescribed intervals or when significant changes occur within your environment. For the purpose of meeting the Framework requirement for certification, you must review your self-assessment every 3 years and submit evidence to the ATO. Where you have had a significant change in your environment which affects the controls you have addressed as part of your self-assessment, you are required to submit a revised version to the ATO as soon as possible.

IRAP

The ASD’s Information Security Registered Assessors Program (iRAP) accredits ICT professionals to assess organisations against the Australian Government’s Information Security Manual. An iRAP assessment will include the following areas:

- Information Security Policy
- Threat Risk Assessment
- System Security Plan
- Security Risk Management Plan
- Incident Response Plan
- Standard Operating Procedures
- Statement of Applicability

ISO/IEC 27001

ISO 27001 is generally completed at the organisational level.

All controls need to be answered, with notes next to each control as to what you do or why the control does not apply to you. We don't expect you to be compliant with all the controls this will be dependent on your organisation's operating model and the architecture of your product.

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 you do to manage the control or if a control doesn't apply to your product why it doesn't apply. We don't expect you to be compliant with all standard 2 controls this will be dependent on your products 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 which are addressed 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 the most suited to IT service providers.

Evidence required

- Completed documentation demonstrating your conformance with the requirements (full control suite) of one of the approved security standards including comments on why certain controls may or may not be applicable to your organisation and how controls that do apply are addressed

Notes

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

Certification (Independent assessment)

The certification requirement seeks to provide the ATO with a level of assurance that you have robust security practices in place across your organisation. This is done by way of attaining independent assessment against one of the below standards:

- iRAP
- ISO/IEC 27001

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

The ATO are unable to prescribe which of the above methods you should use or provide links to them. The choice of what standard to certify against should be made on the basis of suitability to your organisation.

We don’t expect you to be compliant with all the controls of your chosen standard as this will be dependent on your organisation’s operating model and the architecture of your product. We also acknowledge there may be areas where you don’t fully meet a control but have indicated that you will work to address the gap over time.

Your independent certification should be reviewed at prescribed intervals or when significant changes occur within your environment. For the purpose of meeting the Framework requirement for certification, you must maintain your certification on going. This evidence needs to be supplied to the ATO. Where you have had a significant change in your environment which affects the controls you have addressed as part of your certification, you are required to submit a revised version to the ATO as soon as possible.

IRAP

The ASD’s Information Security Registered Assessors Program (iRAP) accredits ICT professionals to assess organisations against the Australian Government’s Information Security Manual. An iRAP assessment will include the following areas:

- Information Security Policy
- Threat Risk Assessment
- System Security Plan
- Security Risk Management Plan
- Incident Response Plan
- Standard Operating Procedures
- Statement of Applicability

ISO/IEC 27001

ISO 27001 is generally completed at the organisational level.

All controls need to be answered, with notes next to each control as to what you do or why the control does not apply to you. We don’t expect you to be compliant with all the controls this will be dependent on your organisation’s operating model and the architecture of your product.

Evidence required

- Completed documentation demonstrating your conformance with the requirements (full control suite) of one of the approved security standards outlined above.
- Statement of Applicability
- Letter of Compliance
- Copy of certificate upon completion of independent certification

Conditional Approval

Where you are undertaking independent certification, you may be eligible for conditional approval where this is the only requirement outstanding. This is due to the timeframe to attain certification being heavily reliant on a third party. Evidence will need to be provided that you have engaged a relevant certifying body to perform the independent assessment against either:

- iRAP
- ISO/IEC 27001

Evidence required

- Letter of Intent to procure service
- Letter of Engagement with a start date, completion date, scope of work and assessor details

Notes

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

Supply chain visibility

The supply chain visibility requirement seeks to annotate the entities and their functional roles involved in the transmission of information from the system which generates the payload through to the ATO. This requirement is only relevant where your product or service does not directly connect to the ATO and the payload is not encrypted.

Evidence required

Until a supply chain visibility solution is available, DSPs are required to provide the business details of the participants in the supply chain including:

- Entity name
- ABN
- Service provider role or function

Notes

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 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 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)

These requirements are an interim measure only and may change when the supply chain visibility solution is available.

Data hosting

This requirement seeks to limit the risk of access to taxation and superannuation related information by individuals no authorised to access – including foreign actors.

Where you use a hosting provider you will need to provide their details to the ATO. The use of an ASD certified hosting environment is recommended but not mandatory.

Evidence required

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

Additional conditions for offshore data hosting

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

Where there is a compelling reason for storing data outside of Australia you must consult with the ATO to ensure that the impact has been adequately addressed. The ATO can provide advice on jurisdictional constraints. As part of the consultation DSPs must demonstrate they have considered the jurisdictional constraints.

The ATO’s preference is for all redundancy locations to mirror those of the primary production environment. Where there are strong encryption controls and alignment to the APRA guides CPG 235 – Managing Data Risk and SPG 231 – Outsourcing, you may consult with the ATO on suitability of redundancy hosting arrangements in an offshore location. Applications will be reviewed on a case by case basis.

Consistent with APRAs Cross Industry Prudential Practice Guide CPG 235, the 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 APRAs Prudential Standard Guide SPG 231, the ATO expects that DSPs would complete a risk assessment against the below risks and steps to mitigate identified risks:

- 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 you as the DSP
- compliance (legal) risk — the 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 — the risk that your ability as a DSP to enforce the offshoring agreement may be limited or completely negated
- access risk — the risk that the 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 — the 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.

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

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 (e.g. clients of tax practitioners, employees, etc) on where and how their data is being managed.

Multi-Factor Authentication (Products/services controlled by the client)

This requirement seeks to minimise the opportunity for unauthorised users to access taxation or superannuation related information.

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 user’s voice.

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).

Further information on each method can be found at ACSC Protect: Multi-factor authentication (PDF)

Although MFA is not a mandatory requirement for products or services which are controlled by the client, the adoption and implementation is highly recommended.

Evidence required

- User manual, user description or instruction paired with screen shots of the user interface

Notes

- End users are those individuals, external to the DSP, who actually use the product or service.
- DSP staff are those staff (including contractors) working for or on behalf of the DSP.
- The ATO may consider exceptions to mandatory MFA for end users of DSP hosted products/services in extenuating circumstances.
- Where the transaction is authenticated within a machine to machine interaction, multi-factor authentication (MFA) is not applicable.
- Tokens or temporary credential should be isolated to an individual device and expire once used. Any token or temporary credential should expire within 24 hours.
- DSPs that have not implemented MFA, should consider implementing passphrase management, account lockout and resetting passphrase practices described in the Information Security Manual pg 195.

Multi-Factor Authentication (Products/services controlled by the DSP)

This requirement seeks to minimise the opportunity for unauthorised users to access taxation or superannuation related information.

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 user’s voice.

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).

Further information on each method can be found at ACSC Protect: Multi-factor authentication (PDF)

The requirements for MFA are determined by the your setup in combination with the type of user and access to other individuals or entities data.

By mandating the use of MFA in your product, additional security is added up front to mitigate the risk of unauthorised access. The following circumstances are examples of when MFA is mandatory (note: this is not an exhaustive list):

- End users who can access taxation or superannuation related information of other entities or individuals (e.g. tax agents, employers)
- DSP staff with access taxation or superannuation related information. This position applies unless the DSP can adequately demonstrate that the internal user does not perform a privileged administration role (system / database level) and the full range of compensating controls specified within the Information Security Manual control material (pages 192 – 195) have been suitably implemented.

The following circumstances are examples of when MFA is not mandatory but is highly recommended (note: this is not an exhaustive list):

- End users that only have access their own information and do not have access to taxation or superannuation related information of other entities or individuals. (E.g. employees accessing employee portals)

Evidence required

- Screenshot of MFA solution paired with user description

Notes

- End users are those individuals, external to the DSP, who actually use the product or service.
- DSP staff are those staff (including contractors) working for or on behalf of the DSP.
- The ATO may consider exceptions to mandatory MFA for end users of DSP hosted products/services in extenuating circumstances.
- Where the transaction is authenticated within a machine to machine interaction, multi-factor authentication (MFA) is not applicable.
- Tokens or temporary credential should be isolated to an individual device and expire once used. Any token or temporary credential should expire within 24 hours.
- DSPs that have not implemented MFA, should consider implementing passphrase management, account lockout and resetting passphrase practices described in the Information Security Manual pg 195.

Security monitoring practices

This requirement seeks to detect and respond to cyber-attacks, channel misuse and business threats. Monitoring is a joint responsibility between the ATO and you as the DSP. Where relevant you need to be able to demonstrate that you scan your environment for threats and that you take appropriate action where you detect anomalies.

Evidence required

Network / infrastructure layer - relevant combinations of:

- screen shots of an intrusion detection system or firewall that generates alerts . If a DSP uses a third party a screenshot from within the solution showing the monitoring capabilities, dashboard etc.
- photos of your Security information and event management dashboard
- If leveraging off a cloud provider you can provide either an invoice or screenshot from within the environment showing the type of monitoring captured.

Application layer – relevant combinations of:

- screen shots of the function page in the application, and
- reports from the backend system.

Transaction (data) layer – relevant combinations of:

- reports from the backend system
- Screenshots of an anomaly detection system.

Sending Service Providers (SSPs)

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

Evidence required

- Intended business model (ie will the service be offered to market)
- Functional role(s) within the value chain
- Services that will be offered (eg 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