Australian Government
Australian Taxation Office

Digital Service Provider (DSP) Operational Security Framework (OSF)

Requirements for Digital Services - Summary of Changes

Presented by:
Diana Porter
DSP Operational Framework Lead

August 2021

Summary of Changes - DSP OSF Controls

The table below represents Operational Security Framework (OSF) controls and a summary of changes agreed to by members of the OSF DSP and Industry focus groups. A whole of OSF working group meeting was held 11 June 2021 to discuss, agree and finalise changes.

*Req = Requirements

DSP Control Requirement	Summary of Change	Clarify Req*	Added Option	Uplift Req*	New Req*
Audit Logging	• Update to provide timeframe, logs must be kept for a minimum 12 months.			●	
	• Clarified audit logging functionality, software must enable traceability of user access and actions through audit logs e.g. who and when logged in, what they viewed and or changed.	●			
	• General improvements made to supporting guidance.	●			
Certification	• Inclusion of ISO 27002 and ISO27017 including NIST to support smaller DSPs in undertaking self certification.		●		
	• General improvements made to supporting guidance.	●			
Data Hosting	• No change to control, general improvements made to supporting guidance.	●			
Encryption	• Clarified use of encryption protocol, all DSPs must use TLS 1.2 or higher.	●			
Entity Validation	• Entity Validation is a new control and ensures the consumer/user of a commercial software product is a legitimate business and has a genuine need to access a DSPs software. The consumer/user must have a valid contact person with contact details, e.g. email and phone.				●
Multi-factor Authentication	• All cloud environments must have MFA in place to access any data in scope of the DSP OSF.				●
	• Remember me functionality limited to 24 hours.			●	
	• Shared logins are not permitted, and need to be blocked by the DSP.			●	
	• Authenticator Apps can be used e.g. Microsoft, Symantec VIP or Google Authenticator with DSPs demonstrating enforcement.	●			
	• MFA should not include Google/Microsoft/Facebook credential to sign in.	●			
	• Use of enterprise SSO require technical assessment and approval by the ATO.	●			
	• General improvements made to supporting guidance.	●			
Personnel Security	• No significant change to the control, general improvements made to supporting guidance.	●			
Security Monitoring	• Control uplifted to include security monitoring for all DSP controlled environments.	●			
	• General improvements made to supporting guidance.	●			
Supply Chain	• No change to control, general improvements made to supporting guidance.	●			
	• ATO not progressing payload encryption at this stage (remains a future work item).	●			
OSF Process	• Change of name to DSP Operational Security Framework.	●			
	• Inclusion to maintain the privacy and security of a DSPs unique product ID.	●			
	• Streamlined annual review procedures	●			
	• Updated Scope to include Accounting, Payroll and Business Registry		●		
	• Improved security incident reporting processes		●		
	• Proposed knowledge hub content (Online Services for DSPs) to support understanding and completion of OSF		●		

Detail of Changes – Controls

The following tables represent the OSF controls and a summary of changes agreed to by members of the OSF DSP and Industry focus groups.

DSP Control Requirement	Prior Version	New Requirement	Type of change
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. You should consider your environment and what logging should be implemented and ensure that the logging records include the 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)). Evidence required •Sample of a dummy audit log in CSV format. •A data dictionary that describes the data attributes and maps against key audit log components.	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 time period. Evidence required DSPs must provide dummy or authentic (sensitive information redacted) access and event logs 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 support this requirement. 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	• **Uplift of control** • **Improved guidance**
Certification	The self-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-certifying against one of the below standards: • iRAP • ISO/IEC 27001 • SOC2 or • OWASP ASVS 3.0 or latest version	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: • iRAP • ISO/IEC 27001 • ISO/IEC 27002 • ISO/IEC 27017 • SOC2 • OWASP ASVS 3.0 or latest version • NIST	• **New option** • **Improved guidance**

Detail of Changes – Controls

DSP Control Requirement	Prior Version	New Requirement	Type of change
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.	• No change to control, general improvements made to supporting guidance. • 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.	• **Improved guidance**
Encryption	You need to provide evidence that your product or service utilises TLS 1.3 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 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 1.3 or HTTPS being enforced • Screenshots from within SSP portal configuration page showing DSP as a linked entity.	To protect the confidentiality and integrity of Taxation, Accounting, Payroll and Superannuation information in transit. DSPs need to provide evidence of an approved protocol TLS 1.2 or higher is used. As per ACSC Guidelines for using Cryptography and Secure Cipher Suits and Annex A of ACSC Implementing Certificates. 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.	• **Improved guidance** • **Uplift of control**
Entity Validation	Entity Validation did not exist in prior version.	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 DSPs need to provide evidence that demonstrates entity validation is in place as part of the product registration/purchase process	• **New control** • **Improved guidance**

Detail of Changes – Controls

DSP Control Requirement	Prior Version	New Requirement	Type of change
Multi-Factor authentication	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 your setup in combination with the type of user and access to other individuals or entities data. Although MFA is not a mandatory requirement for products or services which are controlled by the client, the adoption and implementation of MFA is highly recommended. For DSP controlled products or services the following circumstance is an example of when MFA is not mandatory but is highly recommended (note: this is not an exhaustive list). Example: End users or external users that only have access to 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) Example: Internal users who access tax and super data and the DSP can adequately demonstrate that the internal user does not perform a privileged administration role (system / database level) and that good passphrase practices including single factor authentication controls, account lockouts, resetting passphrases, session and screen locking as described in the Australian Government Information Security Manual (ISM) are implemented.	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. • 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. • 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 must contact the DPO to discuss your proposed solution. • Use of enterprise SSO logins require technical assessment and approval by the ATO.	• **Uplift of control**

Detail of Changes – Controls

DSP Control Requirement	Prior Version	New Requirement	Type of change
Multi-Factor authentication (continued)	The following circumstances are examples of when MFA is mandatory (note: this is not an exhaustive list): Example: DSP staff who perform a privileged user role as defined in the Australian Government Information Security Manual (ISM) with access taxation or superannuation related information. Enterprise Customers By exception, DSPs must seek advice from the ATO on the use of Single Sign On (SSO) for enterprise customers that access a DSP's system from behind their enterprise firewall. SSO must be controlled by the DSP and only enabled for a customer where the below controls are in place. In considering whether to support SSO for their customers, DSPs must ensure that that the customer: • is an enterprise that has control over the access management solutions e.g. (does not use social media as a sign in) • has strong encryption in place e.g. TLS1.2 • has a password or passphrase management policy, covering length and complexity including salt, hashing • enforces brute force lockout Note • 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 good passphrase practices including single factor authentication controls, account lockouts, resetting passphrases, session and screen locking as described in the Australian Government Information Security Manual (ISM) • A privileged user is defined as a user who can alter or circumvent a system's security measures – this may include the capability to modify system configurations, account privileges, audit logs, data files or applications. Evidence required User manual, user description or instruction paired with screen shots of the user interface .	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 • Enforcement of 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. • Session time-out occurs after 15 minutes. • 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 All the requirements below: • User description paired with screen shots of MFA workflow; and • User access controls including remember me, session time-out, brute force lockouts; and • Password or access control policy.	• **Uplift of Control**

Detail of Changes – Controls

DSP Control Requirement	Prior Version	New Requirement	Type of change
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	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 (one or two 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	• **Improved Guidance**
Security Monitoring	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.	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.	• **Uplift of control** • **Improved guidance** • **Control uplifted to include security monitoring for DSP cloud environment**

Detail of Changes – Controls

DSP Control Requirement	Prior Version	New Requirement	Type of change
Supply Chain	The supply chain visibility requirement seeks to identify the entities and annotate 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. 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 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 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 (e.g. CSV or encrypted).	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. ATO not progressing payload encryption at this stage (remains a future work item).	• **Updated guidance**
Category E	Did not exist in prior version	Category E • Commercial productor service controlled by the DSP or the client, and • No risk APIs regardless of unique client records *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, Medium or High-Risk APIs with less than 10,000 unique client records	• **New option**

Detail of Changes – Controls & Process

DSP Control Requirement	Prior Version	New Requirement	Type of change
Document Structure	Contents 	Contents 	• **Updated guidance**
DSP categories	Categories did not exist in prior version	• Re-classification of information and creation of 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, Medium or High-Risk APIs with greater than 10,000 unique client records **Category E**: • Commercial 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, Medium or High-Risk APIs with less than 10,000 unique client records.	• **Updated guidance**

Detail of Changes – Controls & Process

DSP Control Requirement	Prior Version	New Requirement	Type of change
OSF Process	• Original annual review process The ATO will conduct an annual review of all DSPs who have been approved under the Framework. During this process, DSPs will be required to revisit the Framework requirements and provide assurance of their compliance. DSPs will be provided with a review date as part of their approval – typically 12 months after approval. One month prior to the review date, the DPO will remind the DSP of the review. As part of the review, DSPs will need to confirm if there have been any changes to their business or product environment. Where this is the case, the DSPs may need to provide additional information in line with the requirements. Where there have not been any changes in the business / product environment, DSPs will need to provide formal confirmation.	• Streamlined annual review procedures • Improved security incident reporting processes • Proposed knowledge hub content (Online Services for DSPs) to support understanding and completion of OSF	• **Uplift of control** • **Improved guidance** • **New option**
Product ID	(Mandatory) DSPs with multiple products will need one product ID per product. 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 or sending service providers.	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.	• **Improved guidance**

Detail of Changes – Process

DSP Control Requirement	Prior Version	New Requirement	Type of change
Reporting Security Incidents	Monitoring and data breaches Monitoring is considered a joint responsibility between the ATO and DSPs. The ATO conducts monitoring at the network, application and transaction layers; if anomalies or areas of concern are identified, the ATO will work with the DSP to address and limit the damage of the threat. This may include increasing the requirements a DSP needs to meet or introducing additional requirements. The ATO will generally contact a DSP before taking action unless exceptional circumstances apply. A data or identity security breach may include: • Identity details being accessed or seen by an unauthorised third party • Identity details being lost or stolen due to illegal access by a third party activity (e.g. common online threats such as malware, spyware or ransomware). • Mistakenly providing information to the wrong person, for example sending details out to the wrong email address. • A breach of a third party product or service which integrates with a DSP's API (application programming interface). Where a DSP identifies a breach through their own monitoring controls or have been informed directly by a client or third party, the ATO must be notified immediately. This can be done via your account manager, Online Services for DSPs or DPO@ato.gov.au to ensure appropriate action can be taken. In order for the ATO to take action to limit the damage and identify the source of the threat, the following information is requested: • appropriate contact person (specialist IT security/fraud representative) • nature of the incident • number of affected records • date and timestamp • session ID reference • host Services (Internet Service Provider)/IP address • device ID (ESID) if available • TFN information • non-TFN information (name/address/biographical information) • product name and type (desktop or cloud) • what format the data was in (e.g. CSV or encrypted).	Reporting Security Incidents A security incident occurs when personal information an entity holds is subject to unauthorised access or disclosure. This may be caused by a failure in security systems, information handling, human error or malicious action. Security incidents 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 or threat to clients and systems. 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 in order for the ATO to mitigate damage or threats to clients and systems. A security incident may include: • Identity details being accessed or viewed by an unauthorised 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 the wrong person 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 Security Incident A security incident should be reported to DPO immediately from the time a DSP is made aware of the incident, the sooner the information is provided, the quicker ATO can implement preventative action. DSPs can provide information in stages whilst undertaking their own internal investigations. Note: Immediately is as soon as practicable and should be within a few hours. In some circumstances it would be acceptable for a breach notification to be provided to the DPO within 72 hours. This is where security incidents have been contained within the DSP environment through corrective action e.g. a compromised username and password has been reset, including no compromise to the account or information. How to Report an Incident DSPs must report security incidents via the incident report form within Online Services for DSPs and/or via the SBR service desk on 1300 448 231	• **Updated guidance**

Detail of Changes – Controls & Process

DSP Control Requirement	Prior Version	New Requirement	Type of change
Reporting Security Incidents (continued)	Awareness of other obligations In addition to the requirements of the Framework, 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 the 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	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 take action and limit the harm caused by a security incident, the following information is required (when known): • Appropriate contact person (specialist IT security/fraud representative) • Nature of the incident • Number of affected records • Date and timestamp • Session ID reference • Host Services (Internet Service Provider)/IP address • DeviceID (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 incident 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 an incident has been reported or identified ATO may take the following actions: • Switching off an impacted product or API • Suspend or delay access to APIs • Apply security measures to protect client accounts •Provide communication direct to a user of an impacted product. 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.	• **Updated guidance**

Detail of Changes – Controls & Process

DSP Control Requirement	Prior Version	New Requirement	Type of change
Scope	Where a DSP provides a software product or service that reads, modifies or routes any tax or superannuation related information and that product performs a role in the supply chain then that product or services is within scope of the Framework. This includes DSPs that use an intermediary (such as a gateway or sending service provider) to interact with the ATO. More specifically, the DSP Operational Framework applies to software products and services that provide any of the below functionality: • Business and tax accounting services e.g. activity statements and income tax returns • Payroll and employer services e.g. Single Touch Payroll reporting • Superannuation services e.g. Fund member rollover and reporting. Note: Super services may have additional requirements above and beyond the Framework. Due to a continually changing digital environment the requirements for DSPs will be subject to future changes based on risk.	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. It may also include: 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.	• **Updated guidance** • **New options**
Third Party Add-On	DSPs with add-on marketplaces This requirement seeks to identify DSPs that allow third-party add-ons to connect to their software via an API and what if any security controls are in place to govern their access. For this purpose SSPs/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 If you are a DSP with an add-on marketplace you will need to provide additional information. Evidence required • Details on the security standard you adopt to govern your add-ons. Whilst the ATO does not prescribe or mandate the security standard you apply to your 3rd party add-ons, we can recommend the ABSIA Security Standard for Add-on Marketplaces (SSAM) as a baseline. • List of your third-party add-ons with more than 1,000 Australian business connections and/or a connection to an Australian tax agent/practice. The list should include: o The third-party developers name o Hyperlink to their product	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. Evidence required • Information and details of the security standard a DSP adopts to govern their add-ons. Whilst ATO does not prescribe or mandate a security standard a DSP applies to their third-party add-ons; we can recommend the Security Standard for Add-on Marketplaces (SSAM)as a baseline. • A list including the third-party developers name and a hyperlink to their product. 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 more than 1,000 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).	• **Improved guidance**