



# Digital Service Provider (DSP) Operational Security Framework Review

## Working Group Update

Presented by:  
Kylie Johnston  
Director Digital Partnership Office

Diana Porter  
Operational Framework Lead

11 June 2021

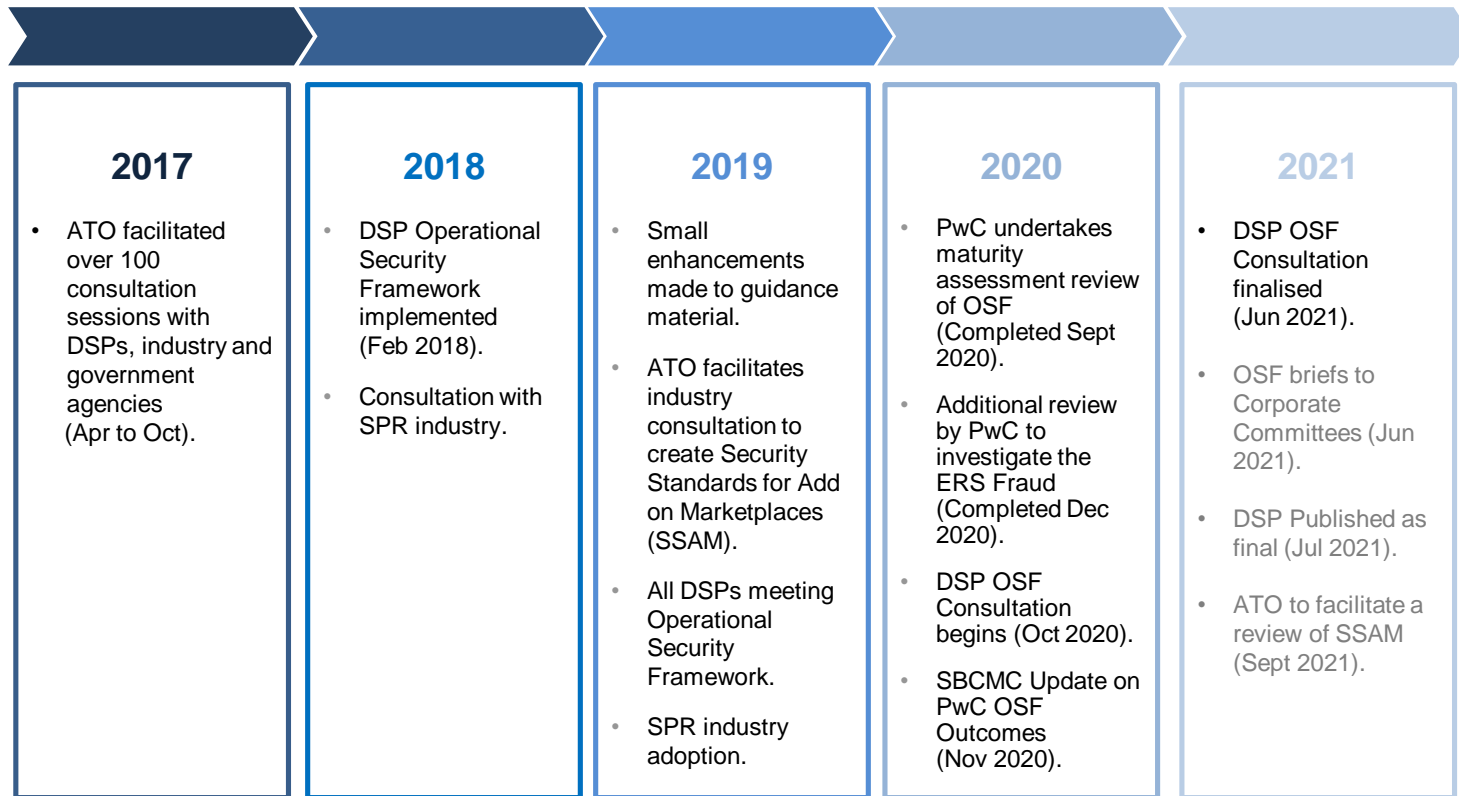


# Operational Security Framework (OSF) Implementation

The DSP Operational Security Framework (OSF) is ATO's approach to recognise and respond to data risks posed by access to ATO Application Processing Interface (API).

OSF consultation commenced in 2017, with requirements implemented in 2018 and a review undertaken throughout 2020/21 based on the expectation of continual evolution.

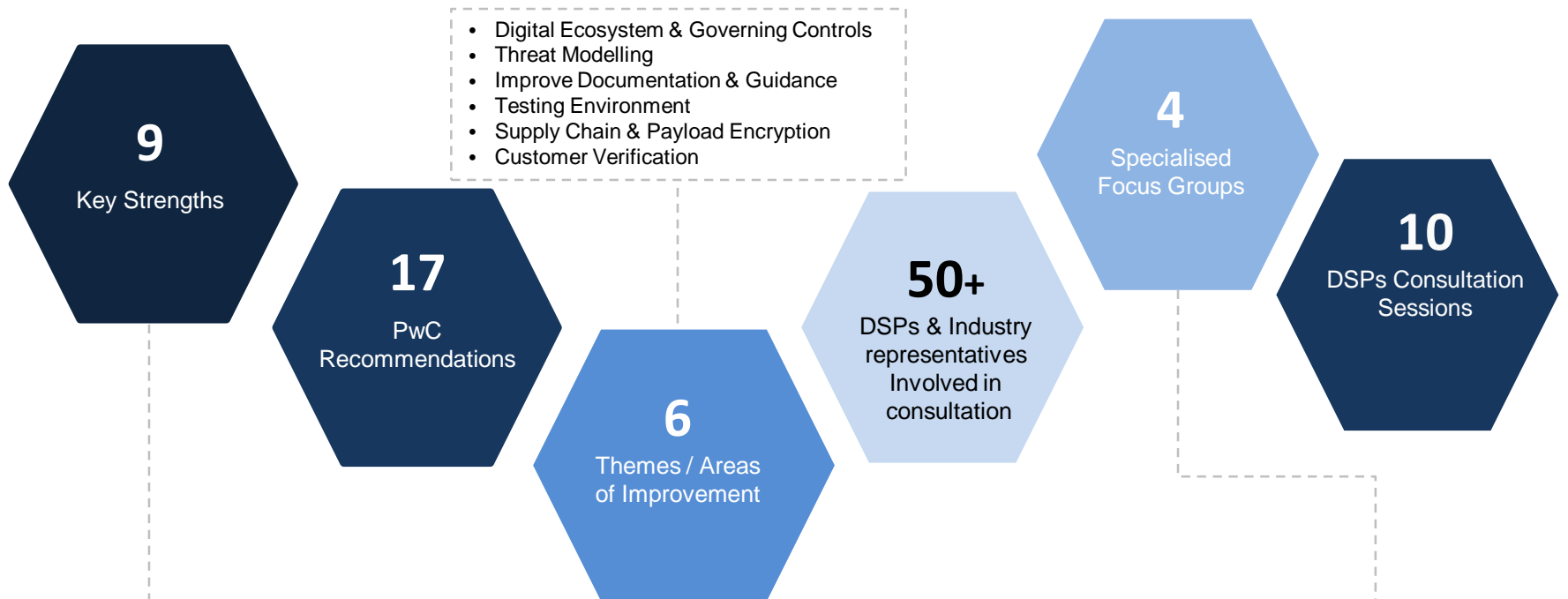
## Roadmap



# Outcomes of PwC Maturity Assessment

PwC undertook a maturity assessment of DSP Operational Security Framework and rated the framework in a maturing state, representing a result of 4 out of a 5 scale rating.

*“It was noted as a very positive result for a framework that has been in operation for only 3 years”.*




<ul style="list-style-type: none"> <li>• <b>Positive compliance</b> due to flexible choice of standards.</li> </ul>	<ul style="list-style-type: none"> <li>• High number of <b>DSPs certifying</b> against ISO/IEC 27001.</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Annual process</b> aligned with Information Security Manual (ISM) expectations.</li> </ul>
<ul style="list-style-type: none"> <li>• DSP lifecycle overview provides relevant and <b>positive security</b> guidance.</li> </ul>	<ul style="list-style-type: none"> <li>• <b>DSPs engaged</b> and understand the importance of the OSF process.</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Security monitoring</b> approach within SBR channels has matured.</li> </ul>
<ul style="list-style-type: none"> <li>• Larger DSPs/ Sending Service Providers <b>advocating</b> for their DSPs or clients.</li> </ul>	<ul style="list-style-type: none"> <li>• Working groups improved the quality and <b>adoption of changes</b> OSF.</li> </ul>	<ul style="list-style-type: none"> <li>• Good <b>guidance</b> provided to DSPs on personnel security checks.</li> </ul>

- Authentication
- Fraud Detection & Monitoring
- Supply Chain & Payload Encryption
- Requirements & Lifecycle Management

# PwC Recommendations

PwC provided 17 recommendations to ATO to explore and work through. A number of the recommendations required internal action only, these have been completed. Some recommendations required exploration through internal and external consultation and remain noted for potential future programs. The remaining items have been consulted with both industry and internal SMEs and have resulted in changes to the OSF requirements and documentation and will be finalised in July 2021.

	Theme	Recommendations
Process & Documentation	Digital Ecosystem & Governing Controls	<ul style="list-style-type: none"> <li>▪ Create end-to-end view of supply chain models, identifying governance controls e.g. OPF, TASA for agents, SSAM for third party DSPs etc. in order to undertake gap analysis of interactions in digital ecosystem.</li> <li>▪ Explore options to include coverage of non SBR services e.g. BDE.</li> </ul>
	Threat Modelling	<ul style="list-style-type: none"> <li>▪ Undertake threat modelling exercises against end-to-end digital ecosystem.</li> <li>▪ Review existing de-whitelisting policy to manage response to cyber risks.</li> </ul>
	Improve Documentation & Guidance	<ul style="list-style-type: none"> <li>▪ Explore improvements to OSF guidance and documentation to support DSPs undertaking self certification including complementary security standards.</li> <li>▪ Explore improvements to OSF guidance and documentation to support encryption in transit protocols and key management plans.</li> <li>▪ Explore improvements to OSF guidance and documentation to support requirements and DSP Questionnaire.</li> <li>▪ Explore improvements to OSF guidance and documentation to support annual review process and notification of DSP product environment changes.</li> <li>▪ Explore feasibility to improve testing processes including the improved non-production test environment.</li> </ul>
	Testing Environment	<ul style="list-style-type: none"> <li>▪ Improve guidance material on retention, preservation of audit logs &amp; breach notification.</li> <li>▪ Expanding security monitoring controls &amp; fraud detection models to all DSP controlled environments.</li> </ul>
Technical Solutions	Supply Chain & Payload Encryption	<ul style="list-style-type: none"> <li>▪ Explore potential technical solutions for supply chain visibility and payload encryption / end to end encryption.</li> </ul>
	Customer Verification	<ul style="list-style-type: none"> <li>▪ Explore opportunities to include customer verification between DSP and their clients in addition to supporting end user clients within software (e.g. tax agent users).</li> <li>▪ Explore responsibility and potential options to identify end user operating through M2M credentials.</li> <li>▪ Explore feasibility of customer verification through DSPs ability to validate through myGovID and RAM.</li> <li>▪ Explore broadening MFA scope client controlled applications (cloud &amp; desktop) &amp; individuals access to own records.</li> <li>▪ Review requirements &amp; guidance of MFA 'remember me' functionality.</li> </ul>



Outcomes  
from individual  
focus groups

# Outcomes: Authentication Focus Group

**Intent of Focus Group:** Identify and explore opportunities to improve authentication.

## Entity Validation

- Entity Validation between DSPs and clients.
- Supporting Customer Verification in software.

## Expansion of MFA

- In client controlled environments (desktop).
- In DSP controlled environments (cloud).

## Improved Guidance & Documentation

- Authentication hardening controls.
- Single Sign On (SSO).

## Outcome Summary

- Entity validation to be undertaken to confirm an entity is a legitimate business with a valid contact person and contact details.
- Entity validation is to be implemented at registration or subscription renewal.
- DSPs are to support customer verification within software.
- MFA has been uplifted to ensure any user accessing any data from within a DSP controlled / cloud environment will require mandatory MFA.
- 'Remember-me' functionality must be limited to 24 hours maximum.
- Uplift of SSO requirement and alignment of standards to ACSC guidelines i.e. SSO token are to be limited to 24 hours of inactivity.

## Next Steps

- DPO will provide additional information including scenarios in a newly created support page within the knowledge hub of OS4DSPs to support adoption or application of the OSF requirements.

# Outcomes: Fraud Detection & Monitoring Focus Group

**Intent of Focus Group:** To improve information security documentation relating to fraud detection and monitoring controls.

## Expanding Security Monitoring

- Explore benefits in expanding scope of security monitoring control to all DSP controlled & cloud environments.

## Preservation and Retention of Log Data

Guidance on:

- Protection, preservation of audit logs.
- Retention periods that align to legislative requirements.
- Accessing information to share in the case of a security incident.

## Breach Notification Guidance

Guidance on:

- Respond to breaches.
- Report a security breach.
- With incident response and fraud investigations.
- With supporting information for clients.

## Outcome Summary

- Security Monitoring will be uplifted to include all DSP controlled cloud environments (there will be no differentiation between the API risk rating or volumes).
- Streamlined guidance on evidence required to better represent the evidence provided by DSPs.
- Audit logging control updated to provide timeframe, logs must be kept for a minimum of 12 months. User access controls to be tightened to enable traceability of user access and actions through audit logs. Shared log-ins are not to be permitted.

Breach notification guidance will have more clarity and an improved process to report security breaches, including:

- Removal of duplicated fields (in online form).
- Removal of fields which have not been used in the past 12 months (in online form).
- Modification of fields to provide clarity of requested information (in online form).
- Updates to documentation to include when, timeframe & how to notify the ATO and what action ATO will take.
- Provide clarity on when a DSP is required to notify of a security incident.
- Provide factors and examples to assist DSPs determine timeframe to report i.e. breach of TFN or bank account.

## Next Steps

- DPO will provide additional information including scenarios in a newly created support page within the knowledge hub of OS4DSPs to support adoption or application of the OSF requirements.

# Outcomes: Supply Chain & Payload Encryption

Explore opportunities to improve integrity of transactions over ATO gateways.

## Supply Chain Visibility

- Governing controls through supply chain.
- Review supply chain solution

## Improved guidance for Encryption

- Encryption in transit
- Encryption at rest
- Encryption key management

## Payload Encryption

- Exploring payload encryption
- Review of current documentation

## Outcome Summary

- **Supply chain visibility** reviewed by DPO. Threat modelling scenarios have been completed against the digital ecosystem and governing controls. DPO will undertake further threat modelling exercise when any new service/product build uniquely differs from the existing DSP OPF scope.
- Provide further clarity and definitions regarding File Transformer and Data Transformer and an updated glossary.

Improved guidance for **Encryption**, including:

- Additional context for cloud solutions that indirectly connect to the ATO. Will be required to provide both public certificates and evidence of indirect connection.
- Additional guidance for encryption at rest. i.e. DSPs can choose to apply this control by either encrypting the disk, container, application or database.
- Providing further clarity and definitions regarding **TLS Standards** and update to glossary.
- Clarity on the type and amount of evidence to be supplied by the DSP and will updates to documentation i.e. 'one of the below' or 'all the below'.
- There will be no change to the technical requirements for **Payload Encryption** e.g. no implementation of payload encryption at this stage.
- Further investigation of payload encryption on hold and DPO will **review in approximately 12 months**.

## Next Steps

- DPO will provide additional information including scenarios in a newly created support page within the knowledge hub of OS4DSPs to support adoption or application of the OSF requirements.



# Outcomes: Requirements & Lifecycle Management

Explore opportunities to improve process, guidance and documentation.

## Supporting guidance for certification

- DSPs with multiple products including certification
- Enhancing certification for DSPs
- Guidance on indirect consumers and third party applications
- Guidance on volume of records

## Guidance and process on DSP Lifecycle Management


- Terms & Conditions relating to data breaches
- Improvements to Letter of Confirmation
- Improvements to Annual Review guidance and process
- Notification of significant changes

## Outcome Summary

- Updated **guidance for certification** for DSPs with multiple products. The scope of certification should cover relevant organisational policies, procedures and data repositories that hold or manage tax or superannuation related information. This will be accepted as evidence when the DSP can assert that each product is covered under the certification.
- DPO will now accept self certification of **ISO 27002, ISO27017 and NIST** as an additional standard to support DSPs.
- **Clarification on volume** of records in glossary i.e. product or service that transmits over 10,000 unique client Taxation, Superannuation, Accounting and Payroll records through ATO digital wholesale services.
- Lifecycle management updates.
- Streamlined annual review procedures.
- Improved security incident reporting processes.

## Next Steps

- DPO will provide additional information including scenarios in a newly created support page within the knowledge hub of OS4DSPs to support adoption or application of the OSF requirements.



# Summary of proposed changes

# Summary of proposed changes

The table below represents OSF controls and a summary of proposed changes agreed to by members of the OSF DSP and Industry focus groups. A whole of OSF working group meeting has been scheduled for 11 June 2021 to discuss and finalise agreed changes with members.

\*Req = Requirements

DSP Control Requirement	Summary of Change	Clarify Req*	Added Option	Uplift Req*	New Req*
<b>Audit Logging</b>	<ul style="list-style-type: none"> <li>Update to provide timeframe, logs must be kept for a minimum 12 months.</li> <li>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.</li> <li>General improvements made to supporting guidance.</li> </ul>			●	
		●			
		●			
<b>Certification</b>	<ul style="list-style-type: none"> <li>Inclusion of ISO 27002 and ISO27017 including NIST to support smaller DSPs in undertaking self certification.</li> <li>General improvements made to supporting guidance.</li> </ul>		●		
		●			
<b>Data Hosting</b>	<ul style="list-style-type: none"> <li>No change to control, general improvements made to supporting guidance.</li> </ul>	●			
<b>Encryption</b>	<ul style="list-style-type: none"> <li>Clarified use of encryption protocol, all DSPs must use TLS 1.2 or higher.</li> </ul>	●			
<b>Entity Validation</b>	<ul style="list-style-type: none"> <li>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.</li> </ul>				●
<b>Multi-factor Authentication</b>	<ul style="list-style-type: none"> <li>All cloud environments must have MFA in place to access any data in scope of the DSP OSF.</li> <li>Remember me functionality limited to 24 hours.</li> <li>Shared logins are not permitted, and need to be blocked by the DSP.</li> <li>MFA cannot include Google/Microsoft/Facebook credential to sign in.</li> <li>Use of enterprise SSO/federated logins require technical assessment and approval by the ATO.</li> <li>General improvements made to supporting guidance.</li> </ul>				●
				●	
				●	
		●			
		●			
		●			
<b>Personnel Security</b>	<ul style="list-style-type: none"> <li>No significant change to the control, general improvements made to supporting guidance.</li> </ul>	●			
<b>Security Monitoring</b>	<ul style="list-style-type: none"> <li>Control uplifted to include security monitoring for all DSP controlled environments.</li> <li>General improvements made to supporting guidance.</li> </ul>			●	
		●			
<b>Supply Chain</b>	<ul style="list-style-type: none"> <li>No change to control, general improvements made to supporting guidance.</li> <li>ATO not progressing payload encryption at this stage (remains a future work item).</li> </ul>	●			
		●			
<b>OSF Process</b>	<ul style="list-style-type: none"> <li>Streamlined annual review procedures</li> <li>Improved security incident reporting processes</li> <li>Proposed knowledge hub content (Online Services for DSPs) to support understanding and completion of OSF</li> </ul>	●			
			●		
			●		

# Operational Security Framework (OSF) proposed scope and transition

The original scope of the DSP OSF has been enhanced to include additional terminology i.e. inclusion of Accounting and Payroll data to provide greater clarification of who needs to meet the requirements.

## 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 or Superannuation data through ATO digital wholesale services.

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

- Connects directly to ATO digital wholesale services.
- Connects indirectly to ATO via a sending service provider (SSP) for payroll services.
- Connects indirectly to ATO via a gateway for superannuation services or Super stream.

It may also include:

- Commercial products significantly modified or white labelled.
- Software products developed for in-house use.
- A software file, for example .CSV, specifically designed to capture payroll data and be uploaded to the ATO via an SSP.

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 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 daily operations.

## Transition and implementation

- For all existing certified DSPs, implementation should be aligned to the next annual review cycle\*.
- For all new DSP OSF submissions, DSPs will need to meet the requirements from the date of publishing.

\*If DSPs are unable to meet the changes by their next annual review date (based on the annual review occurring within 6 months of publishing), they are advised to contact the DPO to discuss their circumstances and implementation timeframes.

## Detail of proposed changes

The table below represents OSF controls and summary of proposed changes agreed by members of the OSF DSP and Industry focus groups. A whole of OSF working group meeting has been scheduled for 1 June 2021 to discuss and finalise agreed changes with members.

DSP Control Requirement	Existing	Proposed changes	Type of change
<b>Audit Logging</b>	<p>This requirement seeks to ensure traceability of access and actions.</p> <p>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:</p> <ul style="list-style-type: none"> <li>• Date and time of the event</li> <li>• Relevant user or process</li> <li>• Event description</li> <li>• Success or failure of the event</li> <li>• Event source e.g. application name</li> <li>• ICT equipment location and identification</li> <li>• Data identifiers (product ID, Tax File Number (TFN)).</li> </ul> <p>Evidence required</p> <ul style="list-style-type: none"> <li>• Sample of a dummy audit log in CSV format.</li> <li>• A data dictionary that describes the data attributes and maps against key audit log components.</li> </ul>	<p>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.</p> <p>Audit logging needs to include:</p> <ul style="list-style-type: none"> <li>• Access and event-based logs.</li> <li>• Users with privileged access must also be identifiable within these logs.</li> <li>• Shared login credentials are not permitted, and each individual user and session will need to be uniquely identifiable through audit logs.</li> <li>• Logs must be kept for a minimum of 12 months.</li> </ul> <p>Evidence required</p> <p>DSPs must provide dummy or authentic (sensitive information redacted) access and event logs which include:</p> <ul style="list-style-type: none"> <li>• Authentication and authorisation</li> <li>• Date and time of the event</li> <li>• Username / identifier</li> <li>• Success or failure of the event</li> <li>• Event description</li> <li>• ICT equipment location and identification</li> <li>• DSPs can provide an Audit log policy to support this requirement.</li> </ul> <p>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.</p>	<ul style="list-style-type: none"> <li>• Uplift of control</li> <li>• Improved guidance</li> </ul>
<b>Certification</b>	<p>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:</p> <ul style="list-style-type: none"> <li>• iRAP</li> <li>• ISO/IEC 27001</li> <li>• SOC2 or</li> <li>• OWASP ASVS 3.0 or latest version</li> </ul>	<p>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:</p> <ul style="list-style-type: none"> <li>• iRAP</li> <li>• ISO/IEC 27001</li> <li>• ISO/IEC 27002</li> <li>• SOC2</li> <li>• OWASP ASVS 3.0 or latest version</li> <li>• NIST</li> </ul>	<ul style="list-style-type: none"> <li>• New option</li> <li>• Improved guidance</li> </ul>

## Detail of proposed changes

DSP Control Requirement	Existing	Proposed changes	Type of change
<b>Data Hosting</b>		<ul style="list-style-type: none"> <li>No change to control, general improvements made to supporting guidance.</li> </ul>	<ul style="list-style-type: none"> <li>Improved guidance</li> </ul>
<b>Encryption</b>	<p>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.</p> <p>Evidence required</p> <p>When directly connecting to the ATO a screenshot of one of the below:</p> <ul style="list-style-type: none"> <li>SSL certificates</li> <li>Showing HTTPS protocol being enforced</li> <li>Call to API</li> <li>TLS handshake protocol being enforced.</li> </ul> <p>When using an SSP/Gateway to indirectly connect to the ATO:</p> <ul style="list-style-type: none"> <li>Licensing agreement or contract for service with SSP</li> <li>Call to the SSP REST API</li> <li>Handshake agreement with SSP showing TLS 1.3 or HTTPS being enforced</li> <li>Screenshots from within SSP portal configuration page showing DSP as a linked entity.</li> </ul>	<p>DSPs need to provide evidence that an approved protocol TLS 1.2 or higher is used as per ACSC Guidelines for using Cryptography and Secure Cipher Suits.pdf are used as per Annex A of ACSC Implementing Certificates.pdf</p> <p>Evidence required</p> <p>All cloud products must provide one of the following:</p> <ul style="list-style-type: none"> <li>Back-end configuration of TLS (e.g. load balancer)</li> <li>SSL labs report for public certificates</li> </ul> <p>All indirectly connecting products must provide one of the following:</p> <ul style="list-style-type: none"> <li>Licensing agreement with SSP</li> <li>Screenshots from SSP portal</li> <li>Screenshot of API call to 3rd party showing TLS protocol.</li> </ul> <p>Note: Desktop products that directly connect to the ATO are not required to provide evidence for this requirement.</p>	<ul style="list-style-type: none"> <li>Improved guidance</li> <li>Uplift of control</li> </ul>
<b>Entity Validation</b>		<p>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. This requirement seeks to prevent unauthorised access to Taxation, Accounting, Payroll or Superannuation related information.</p> <p>Entity Validation establishes that an entity registering to use business, payroll, superannuation or tax software is a valid and registered entity as per the Australian Business Register (ABR) or equivalent.</p> <p>To complete entity validation, a DSP will need to verify the entity against reliable and independent sources, which may include Australian Business Registry Service, ABN Lookup, website/URL, domain specific email addresses or media advertisement.</p> <p>Customers who do not have an ABN, are a student i.e. university/TAFE student using software for their studies/course or are using a product outside DSP Operational Security Framework scope, must have a valid contact person with contact details, e.g. email and phone.</p> <p>Evidence required</p> <p>DSPs need to provide evidence that demonstrates entity validation is in place as part of the product registration/purchase process.</p>	<ul style="list-style-type: none"> <li>New control</li> <li>Improved guidance</li> </ul>

## Detail of proposed changes

DSP Control Requirement	Existing	Proposed changes	Type of change
<b>Multi-Factor authentication</b>	<p>This requirement seeks to minimise the opportunity for unauthorised users to access taxation or superannuation related information.</p> <p>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.</p> <p>The authentication factors can be categorised as:</p> <ul style="list-style-type: none"> <li>• Something you know, such as a password or a response to a security question</li> <li>• Something you have, such as a one-time pin, SMS message, smartcard, or software certificate</li> <li>• Something you are, such as biometric data, like a fingerprint or user's voice</li> </ul> <p>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).</p> <p>Further information on each method can be found at ACSC Protect: Multi-factor authentication (PDF)</p> <p>The requirements for MFA are determined by your setup in combination with the type of user and access to other individuals or entities data.</p> <p>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.</p> <p>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).</p> <p>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)</p> <p>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.</p>	<p>Multi-Factor Authentication (MFA)</p> <p>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.</p> <p>The authentication factors can be categorised as:</p> <ul style="list-style-type: none"> <li>• Something you know, such as a password or a response to a security question</li> <li>• Something you have, such as a one-time pin, SMS message, smartcard, or software certificate</li> <li>• Something you are, such as biometric data, like a fingerprint or user's voice</li> </ul> <p>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).</p> <p>MFA for DSP controlled environments</p> <p>MFA is required for all users of software products that are controlled or hosted by the DSP.</p> <p>This requirement seeks to minimise the opportunity for unauthorised users to access Taxation, Accounting, Payroll or Superannuation related information.</p> <p>Shared login credentials are not permitted, and each individual user and session will need to be uniquely identifiable through audit logs. Shared logins need to be blocked by the DSP.</p> <p>"Remember Me on this device" functionality must be limited to 24 hours.</p> <p>Sign in with Google/Microsoft/Facebook (and other equivalent services) is not permitted without prior approval from the DPO. A DSP wishing to use a Google/Microsoft/Facebook login will need to demonstrate how MFA is enforced as part of login.</p> <p>DRAFT FOR CONSULTATION OFFICIAL EXTERNAL 22</p> <p>Use of enterprise SSO/federated logins (e.g. SAML) requires technical assessment and approval by the ATO on a customer by customer basis.</p> <p>Further information on each method can be found at ACSC: Implementing Multi Factor Authentication</p> <p>DSPs that have not implemented MFA, should consider implementing passphrase management, account lockout and resetting passphrase practices</p>	<ul style="list-style-type: none"> <li>• Uplift of control</li> </ul>

## Detail of proposed changes

DSP Control Requirement	Existing	Proposed changes	Type of change
<b>Multi-Factor authentication (continued)</b>	<p>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:</p> <ul style="list-style-type: none"> <li>•is an enterprise that has control over the access management solutions e.g. (does not use social media as a sign in)</li> <li>•has strong encryption in place e.g. TLS1.2</li> <li>•has a password or passphrase management policy, covering length and complexity including salt, hashing</li> <li>•enforces brute force lockout</li> </ul> <p>Note</p> <ul style="list-style-type: none"> <li>•End users are those individuals, external to the DSP, who actually use the product or service.</li> <li>•DSP staff are those staff (including contractors) working for or on behalf of the DSP.</li> <li>•The ATO may consider exceptions to mandatory MFA for end users of DSP hosted products/services in extenuating circumstances.</li> <li>•Where the transaction is authenticated within a machine to machine interaction, multi-factor authentication (MFA) is not applicable.</li> <li>•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.</li> <li>•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)</li> <li>•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.</li> </ul> <p>Evidence required                      User manual, user description or instruction paired with screen shots of the user interface</p>	<p>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:</p> <ul style="list-style-type: none"> <li>• Disabling of MFA is controlled by the DSP, not their client.</li> <li>• Clients are aligned to requirements of MFA as per the Operational Security Framework.</li> <li>• SSO tokens must be limited to a maximum period of 24 hours.</li> <li>• Encryption in transit between the client's system and software uses as an approved protocol as per the ACSC - Guidelines for using Cryptography e.g. TLS 1.2 or 1.3.</li> <li>• SSO occurs behind the client's enterprise firewall i.e. gateway.</li> </ul> <p>As per ACSC social media sign-on can be used as an authentication factor.</p> <ul style="list-style-type: none"> <li>• Remember me functionality must be limited to 24 hours maximum.</li> <li>• Enforcement of brute force lockouts are applied after a maximum of 5 unsuccessful login attempts.</li> <li>• Credentials are stored separately from the system which grants access.</li> <li>• Confirmation passwords are hashed, salted and stretched.</li> <li>• Session time-out occurs after 15 minutes.</li> <li>• ACSC Authentication Hardening includes additional guidance to support DSPs implementation.</li> </ul> <p>Note: Short Message Service (SMS), are more susceptible to compromise by an adversary than others. As such the ATO recommends utilising an alternative authentication factor when viable to do so.</p> <p>Evidence required                      All the requirements below:</p> <ul style="list-style-type: none"> <li>• User description paired with screen shots of MFA workflow; and</li> <li>• User access controls including remember me, session time-out, brute force lockouts; and</li> <li>• Password or access control policy.</li> </ul>	<ul style="list-style-type: none"> <li>• Uplift of control</li> </ul>



## Detail of proposed changes

DSP Control Requirement	Existing	Proposed changes	Type of change
<b>OSF Process</b>	<ul style="list-style-type: none"> <li>Original annual review process</li> </ul> <p>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.</p> <p>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.</p> <p>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.</p>	<ul style="list-style-type: none"> <li>Streamlined annual review procedures</li> <li>Improved security incident reporting processes</li> <li>Proposed knowledge hub content (Online Services for DSPs) to support understanding and completion of OSF</li> </ul>	<ul style="list-style-type: none"> <li>Uplift of control</li> <li>Improved guidance</li> <li>New option</li> </ul>
<b>Personnel Security</b>		<ul style="list-style-type: none"> <li>No significant change to the control, general improvements made to supporting guidance.</li> </ul>	<ul style="list-style-type: none"> <li>Improved guidance</li> </ul>
<b>Security Monitoring</b>	<p>Security monitoring practices</p> <p>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.</p> <p>Evidence required</p> <p>Network / infrastructure layer - relevant combinations of:</p> <ul style="list-style-type: none"> <li>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.</li> <li>photos of your Security information and event management dashboard</li> <li>If leveraging off a cloud provider you can provide either an invoice or screenshot from within the environment showing the type of monitoring captured.</li> </ul> <p>Application layer – relevant combinations of:</p> <ul style="list-style-type: none"> <li>screen shots of the function page in the application, and</li> <li>reports from the backend system.</li> </ul> <p>Transaction (data) layer – relevant combinations of:</p> <ul style="list-style-type: none"> <li>reports from the backend system</li> <li>screenshots of an anomaly detection system.</li> </ul>	<p>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.</p> <p>You must demonstrate appropriate monitoring of networks, applications and transactions is in place. This requirement seeks to detect and respond to cyber-attacks, channel misuse and business threats. Monitoring is a joint responsibility between the ATO and a DSP. Where relevant a DSP needs to be able to demonstrate that they scan their environment for threats and that a DSP will take appropriate action where a DSP detects anomalies.</p> <p>Evidence required</p> <ul style="list-style-type: none"> <li>Screenshot of an intrusion detection system such as a firewall that generates alerts.</li> <li>Approach to detect anomalies or a screenshot of a security event and incident management dashboard.</li> <li>Intrusion prevention system which protects end points and scans the DSP environment to prevent malicious events.</li> </ul>	<ul style="list-style-type: none"> <li>Uplift of control</li> <li>Improved guidance</li> <li>Control uplifted to include security monitoring for DSP cloud environment.</li> <li>Additionally, general improvements made to supporting guidance.</li> </ul>

## Detail of proposed changes

DSP Control Requirement	Existing	Proposed changes	Type of change
<b>Supply Chain Visibility</b>	<p>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.</p> <p>The functional roles within a supply chain are defined as:</p> <ul style="list-style-type: none"> <li>• Data Collector: Party responsible for the acquisition of data through user interface interaction or APIs</li> <li>• Data Validator: Party responsible for the verification of data types, structures, formats and/or data values</li> <li>• Data Integrator: Party responsible for combining data from multiple sources for use</li> <li>• Data Analysis and Extraction: Party responsible for performing analysis on data to extract a data sub-set or additional derived/calculated data</li> <li>• Data Transformer: Party responsible for change syntactic representation of data</li> <li>• Data Provider: Party responsible for the payload (which may be encrypted)</li> <li>• Data Transmitter: Party responsible for the message with the payload. (e.g. ebMS3/AS4 transmission).</li> </ul> <p>These requirements are an interim measure only and may change when the supply chain visibility solution is available.</p> <p>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:</p> <ul style="list-style-type: none"> <li>•Entity name</li> <li>•ABN</li> <li>•Service provider role or function.</li> </ul>	<p>This requirement is only relevant where your product or service does not directly connect to the ATO and the payload is not encrypted. Supply chain visibility seeks to identify entities and their functional roles involved in the transmission of information, from the system which generates the payload through to the ATO.</p> <p>The functional roles within a supply chain are defined as:</p> <ul style="list-style-type: none"> <li>• Data Collector: Party responsible for the acquisition of data through user interface interaction or APIs</li> <li>• Data Validator: Party responsible for the verification of data types, structures, formats and/or data values</li> <li>• Data Integrator: Party responsible for combining data from multiple sources for use</li> <li>• Data Analysis and Extraction: Party responsible for performing analysis on data to extract a data subset or additional derived/calculated data</li> <li>• Data Transformer: Party responsible for changing representation of data to file format of data (e.g. CSV to XML)</li> <li>• Data Provider: Party responsible for the payload (which may be encrypted)</li> <li>• 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.</li> </ul> <p>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:</p> <ul style="list-style-type: none"> <li>• Entity name</li> <li>• ABN</li> <li>• Service provider role or function.</li> </ul> <p>ATO not progressing payload encryption at this stage (remains a future work item).</p>	<ul style="list-style-type: none"> <li>• Uplifted control</li> </ul>

## Detail of proposed changes

DSP Control Requirement	Existing	Proposed changes	Type of change
<b>Reporting Security Incidents</b>	<p>Monitoring and data breaches</p> <p>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.</p> <p>The ATO will generally contact a DSP before taking action unless exceptional circumstances apply.</p> <p>A data or identity security breach may include:</p> <ul style="list-style-type: none"> <li>•Identity details being accessed or seen by an unauthorised third party</li> <li>•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).</li> <li>•Mistakenly providing information to the wrong person, for example sending details out to the wrong email address.</li> <li>•A breach of a third party product or service which integrates with a DSP's API (application programming interface).</li> </ul> <p>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.</p> <p>In order for the ATO to take action to limit the damage and identify the source of the threat, the following information is requested:</p> <ul style="list-style-type: none"> <li>•appropriate contact person (specialist IT security/fraud representative)</li> <li>•nature of the incident</li> <li>•number of affected records</li> <li>•date and timestamp</li> <li>•session ID reference</li> <li>•host Services (Internet Service Provider)/IP address</li> <li>•device ID (ESID) if available</li> <li>•TFN information</li> <li>•non-TFN information (name/address/biographical information)</li> <li>•product name and type (desktop or cloud)</li> <li>•what format the data was in (e.g. CSV or encrypted).</li> </ul>	<p>Reporting Security Incidents</p> <p>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.</p> <p>Security Monitoring is considered a joint responsibility between the ATO and DSPs. 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. ATO may also identify risks/threats to our systems or client accounts, occurring via a DSP's software. In these circumstances, ATO will contact a DSP before acting unless exceptional circumstances apply.</p> <p>A security incident may include:</p> <ul style="list-style-type: none"> <li>• Identity details being accessed or viewed by an unauthorised third party</li> <li>• 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.</li> <li>• Mistakenly providing information to the wrong person, e.g. sending details to the wrong email address.</li> <li>• A breach of a third-party product or service that integrates with a DSP's API. See guidelines Security Standard for Add-on Marketplaces (SSAM)</li> </ul> <p>When to report a Security Incident</p> <p>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.</p> <p>Note: Immediately is as soon as practicable and should be within a few hours.</p> <p>In some circumstances where security incidents have been contained within the DSP environment e.g. a compromised username and password, with DSP corrective action undertaken such as an account reset, notification to DPO is within 72 hours.</p> <p>How to Report an Incident</p> <p>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.</p>	<ul style="list-style-type: none"> <li>• Updated guidance</li> </ul>

## Detail of proposed changes

DSP Control Requirement	Existing	Proposed changes	Type of change
<p><b>Reporting Security Incidents (continued)</b></p>	<p>Awareness of other obligations In addition to the requirements of the Framework, DSPs need to be aware of their obligations under:</p> <ul style="list-style-type: none"> <li>• Notifiable Data Breach scheme under Part IIIC of the Privacy Act 1988 (Privacy Act).</li> </ul> <p>For further information on the Notifiable Data Breach scheme, please refer to <a href="https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme">https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme</a></p> <ul style="list-style-type: none"> <li>• Australian Privacy Principles, contained in schedule 1 of the Privacy Act 1988 (Privacy Act)</li> </ul> <p>For further information on the Australian Privacy Principles, please refer to <a href="https://www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles">https://www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles</a></p>	<p>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.</p> <p>For ATO to take action and limit the harm caused by a security incident, the following information is required (when known):</p> <ul style="list-style-type: none"> <li>• Appropriate contact person (specialist IT security/fraud representative)</li> <li>• Nature of the incident</li> <li>• Number of affected records</li> <li>• Date and timestamp</li> <li>• Session ID reference</li> <li>• Host Services (Internet Service Provider)/IP address</li> <li>• Device ID (ESID) if available</li> <li>• TFN information</li> <li>• Non-TFN information (name/address/biographical information)</li> <li>• Product name and type (desktop or cloud)</li> <li>• What format the data is in (e.g. CSV or encrypted).</li> </ul> <p>Actions ATO will take post incident notification ATO will take action to protect the integrity and confidentiality of Taxation and Superannuation systems. 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:</p> <ul style="list-style-type: none"> <li>• Apply security measures to protect client accounts</li> <li>• Switching off an impacted product or API</li> <li>• Suspend or delay access to APIs</li> <li>• Provide communication to alert the public of impacted products</li> </ul> <p>Security tips for clients</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• The Office of the Safety Commissioner also provides information for staying safe online.</li> </ul> <p>Awareness of other obligations In addition to the requirements of the DSP OSF, DSPs need to be aware of their obligations under:</p> <ul style="list-style-type: none"> <li>• 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 <a href="https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme">https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme</a></li> <li>• 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 <a href="https://www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles">https://www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles</a>.</li> </ul>	<ul style="list-style-type: none"> <li>• Uplifted control</li> </ul>

